TIETOTURVASUUNNITELMATYÖKALU

Janne Kortelainen

Opinnäytetyö
Tammikuu 2010

Tietoverkkotekniikka
Informaatio teknologia

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t) KORTELAINEN, Janne	Julkaisun laji Opinnäytetyö	Päivämäärä 26.01.2010
	Sivumäärä 49	Julkaisun kieli Suomi
	Luottamuksellisuus ( ) saakka	Verkkojulkaisulupa myönnetty ( )
Työn nimi TIETOTURVASUUNNITELMATYÖKALU		
Koulutusohjelma Tietoverkkotekniikka		
Työn ohjaaja(t) SILTANEN, Jarmo		
Toimeksiantaja(t) Jyväskylän Ammattikorkeakoulu, Jari Hautamäki		

Tiivistelmä

Opinnäytetyössä rakennettiin yhtenäinen kokonaisuus tietoturvasuunnitelman suunnitteluun, implementointiin ja kehittämiseen pienille sekä keskisuurille yrityksille. Luotiin ohjeistus, joka antaa kansantajuisesti kuvauksen erilaisista ratkaisuista sekä mahdollisuuksista, joita yritykset voivat ja tulevat kohtaamaan omaa tietoturvasuunnitelmaa kehittäessään.

Opinnäytetyö pitää sisällään yleiskuvauksen tietoturvallisuudesta, eri käyttäytymismalleista sekä näiden erilaiset vaikutukset yrityksen kokoon ja toimialaan suhteutettuna. Työssä käydään myös läpi yrityksen tietoturvapolitiikkaa koskevat asiat sekä niiden määrittely ja vastuunjako.

Ohjeistus on pääasiallisesti tarkoitettu yrityksille, joilla ei ole aiemmin ollut tai on selkeästi vanhentuneet käyttäytymismallit omassa tietoturvassaan. Työtä on myös rajattu tiettyihin tekniikoihin ja ideologioihin sillä perusteella, että mahdollisilla kohdeyrityksillä ei välttämättä ole resursseja tai halua investoida suuria summia mittaviin ja kalliisiin standardeihin sekä tekniikkaan.

Prosessin aikana työstä hioutui selkeä kokonaisuus tietoturvallisuuden sekä tietoturvasuunnitelman perusteista, ilmaistuna selkeästi ja helposti ymmärrettävästi. Ohjeistus tarjoaa erilaisia vaihtoehtoja ja selityksiä yrityksen itsensä näkökulmasta ja antaa yritykselle avaimet kehittää itse tietoturvallisuuttaan.

Avainsanat (asiasanat)
Tietoturvasuunnitelma, tietoturvapolitiikka, tietoturva, ohjeistus, työkalu

Muut tiedot

Author(s)
KORTELAINEN, Janne

Type of publication
Bachelor´s / Master's Thesis

Date
26.01.2010

Pages
49

Language
Finnish

Confidential

( ) Until

Permission for web publication
( )

Title
INFORMATION SECURITY PLANNING TOOL

Degree Programme
Data Network Technology

Tutor(s)
SILTANEN, Jarmo

Assigned by
JAMK University of Applied Sciences, Jari Hautamäki

Abstract

During the process of the thesis whole and unified instructions were build for planning, implementation and development of information security specially designed for small and medium-sized businesses. The thesis works as a tutorial that gives an easy description of the various solutions and opportunities that companies can and will face in developing their own information security plan.

The thesis includes a general description of the security of information, different patterns of behavior, and their different impacts on firm size and nature in proportion. The thesis will also discuss the company's information security policy matters as well as their definition and the division of responsibilities.

The guide is primarily intended for companies who have not previously had or that have clearly outdated patterns of behavior in their own information security. The thesis is also limited to certain technologies and ideologies on the basis that potential target companies do not necessarily have the resources or do not want to invest huge sums in large-scale and costly standards and technology.

During the process, the thesis formed into a clear package of information security and an IT security plan, expressed in a clear and easily understandable way. The guide provides a variety of options and explanations of the company itself in perspective and gives the keys to the company to develop IT security by themselves.

Keywords
Information, security, planning, tool, guide

Miscellaneous

SISÄLTÖ

KUVIOT

TAULUKOT

1. TYÖN LÄHTÖKOHDAT

Tämän opinnäytetyön tarkoituksena oli antaa perustietoa ja työkaluja tietoturvan kehittämiselle pienissä sekä keskisuurissa yrityksissä. Toimeksianto työn tekemiselle saatiin Jyväskylän Ammattikorkeakoululta, tietoverkkotekniikan yliopettaja Jari Hautamäeltä, Jarmo Siltasen ollessa tukena kehityskeskusteluissa. Jyväskylän Ammattikorkeakoulu on kansainvälinen ja monialainen korkeakoulu, joka on jaettu eri koulutusyksikköihin, eri osaamisalueiden mukaan. Teknologiayksikkö tarjoaa opetusta ICT, konetekniikka, logistiikka, luonnonvara ja rakentamisen opintoihin eri puolilla Jyväskylää. Näistä ICT keskittyy Jyväskylän Lutakon alueelle, IT-dynamoon, jossa on mahdollista opiskella mm. tietoverkkotekniikkaa, ohjelmointia sekä automaatiotekniikkaa.

Työn tavoitteena oli luoda ohjeistus toimivan tietoturvan kehittämiseen ja implementointiin niin uusille, kuin jo olemassa olevillekin yrityksille, kohdistuen kuitenkin pieniin sekä keskisuuriin yrityksiin. Tavoitteena on luoda opas, jota voisi hyödyntää sellaisenaan yrityksissä, jotka haluavat aloittaa tai uudistaa tietoturvakäytänteitään nykypäivää vastaavalle tasolle. Työssä on myös pyritty luomaan kestävät käytänteet, jotka eivät ole sidottu liian vahvasti tämän hetkiseen tekniikkaan, vaan periaatteet toimisivat vielä monen vuoden kuluttuakin, tekniikan vaihtuessa ja uusien prosessien kehittyessä.

Menetelmissä otettiin huomioon erilaiset kustannustehokkuuteen liittyvät tekijät ja pyrittiin rakentamaan tietoturvaa yrityksen tuotannolliselta kannalta siten, ettei tuottavuus kärsisi tietoturvallisten käytäntöjen implementoinnista. Erilaisten toimintatapojen kautta on luotu myös mahdollisuuksia toteuttaa tiettyjä toimenpiteitä eri tavoin, mahdollistaen näin joustavat investoinnit kohdistuen laitehankintoihin sekä aineettomaan omaisuuteen.

Tietoturvapolitiikkaa kuvataan yrityksen johdon, mutta myös tuotannosta vastaavien työntekijöiden kannalta mahdollisimman yksiselitteisesti ja selkeästi. Riskianalyysin toteuttamisessa perehdytään yrityksen toimialasta ja koosta johtuviin määrittelyihin, yleisiin käytänteisiin sekä erilaisiin, vaihtoehtoisiin tapoihin toteuttaa järjestelmiä.

2. TIETOTURVALLISUUS

2.1 Yleistä tietoturvasta

Tietoturvassa on kyse koko yrityksen tai yhdistyksen toiminnan turvaamisesta niin tahallisilta kuin tahattomiltakin riskeiltä. Tietoturvan tehtävänä on minimoida sekä aineelliset että aineettomatkin tuhot ja häiriöt, kuten tietomurrot, laitevarkaudet ja tietojen kalastelu. On tärkeää ottaa huomioon, ettei tietoturvaa saa pelkästään suojautumalla fyysisten lukkojen ja esteiden taakse, vaan täytyy myös tiedostaa riskit, jotka voivat aiheutua tahattomistakin ja inhimillisistä virheistä tietoa jaettaessa.

Nyky yhteiskunnassa tietoa on valtavia määriä ja koko ajan sitä tulee lisää. Tietoa säilytetään ja kerätään fyysisesti kuten paperille arkistoihin, mutta yhä enemmän tietoa kerätään ja tallennetaan tietokoneilla kovalevyille, optisille levyille ja nauhoille. Kaikki tämä kerätty tieto täytyy suojata asianmukaisesti ja oikeilla periaatteilla. Näiden erilaisten säilytystapojen takia on kuitenkin ehdottoman tärkeää ottaa huomioon niiden erilainen suojaaminenkin. Fyysiset paperiarkistot voidaan suojata järeillä lukoilla, mutta mitä tapahtuu esimerkiksi tulipalon sattuessa? Palvelimien kovalevyille taas voidaan tallentaa määrättömästi tietoa ja palvelimetkin voidaan suojata lukkojen taakse, mutta mitä jos varas tai hakkeri pystyykin murtautumaan palvelimelle tarvitsematta olla edes saman maan rajojen sisäpuolella? Näihin erilaisiin uhkiin ja niin fyysiseen kuin aineettomaankin turvallisuuteen voidaan varautua ennalta ja pitkälle ennalta ehkäistä monet huolellisella suunnittelulla. Tätä suunnittelua kutsutaan tietoturvasuunnitelmaksi sekä politiikaksi.

Tietoturva vaatii jatkuvaa kehittämistä ja jatkuvaa sitoutumista toiminnan ylläpitämiseksi. Projektien läpivienti, riittävä koulutus sekä asianmukainen raportointi ovat askel kohti toimivaa ja tietoturvallista yritystoimintaa, joka takaa jatkuvuuden myös tulevaisuudessa. Mikäli tietoturvallisuuteen suhtaudutaan yrityksessä kertainvestointina, on mahdollista, että muutama kuukausi, ehkä vuosikin menee ”ihan hyvin”, mutta mikäli tietoturvaa ei kehitetä, eikä sen toimintaan panosteta riittävällä tasolla jatkuvasti, menevät investoinnit täysin hukkaan. Päivittämätön tietoturva on sama kuin sitä ei olisi ollenkaan. Onkin siis ensiarvoisen tärkeää viedä ajatus organisaation johtotasolle asti siitä, että kehittyvä ympäristö on toimiva ympäristö, joka

heijastuu perinteisestä yritystoiminnasta aina käytännön työtehtäviin ja tietoturvalliseen käyttäytymiseen. Kun yrityksen johtoryhmä, tietoturvavaltuutettu sekä käyttäjät saadaan perehdytettyä ajatukseen kehittyvästä tietoturvasta ja sen tarpeellisuudesta, uusien tekniikoiden ja menettelytapojen implementointi helpottuu mahdollistaen toimivien ratkaisujen luomisen päivittäiseen käyttöön niin tuotannossa kuin dokumentoinnissa ja johdonkin osalta.

2.2 Menetelmiä

Tiedon varastamiseen, väärinkäyttämiseen sekä keräämiseen on olemassa monenlaisia eri menettelytapoja, joista monet ovat hyvinkin vanhoja ja edelleen varsin toimivia, mutta toiset taas uusia, ja lisää tulee koko ajan. Tietoa ei välttämättä ole helpoin varastaa, mikäli se säilytetään ainoastaan fyysisenä lukkojen takana, mutta se ei toisaalta ole myöskään sitä tarvitsevien tahojen käytettävissä helposti.

Erilaisiin menetelmiin on olemassa kaksi pääasiallista osa-aluetta: phishing ja tietomurrot. Phishingillä tarkoitetaan tiedon kalastelua, jossa ei välttämättä tapahdu edes mitään rikosta. Phishing on vanhin ja edelleen toimivin tapa saada tietoa esimerkiksi suoraan kysymällä haluttua tietoa yrityksen työntekijältä. Taitava rikollinen voi esiintyä jonain toisena henkilönä helposti vaikka puhelimen välityksellä tai jopa paikan päällä ja tietäessään, että tälle henkilölle luovutetaan paljon arkaluonteista materiaalia. Rikollinen voi saada jopa käyttäjätunnuksia ja salasanoja käyttöönsä ja näin päästä suoraan käsiksi yrityksen tietoihin joutumatta tekemään varsinaista murtautumista.

Phishingiä voidaan harjoittaa käytännössä missä vain. Esimerkiksi varas pyrkii ystävystymään jonkun yrityksen työntekijän kanssa, joka tietää paljon yrityksen toiminnasta ja vaikka oluttuopin äärellä lopummalla iltaa vaivihkaa kysellä, kuin ohimennen yrityksen toiminnasta ja tietoa. Monet ihmiset kertovat mielellään salaisiakin tietoja, mikäli tuntevat olonsa turvalliseksi ja etenkin alkoholin vaikutuksen alaisena.

Toisena esimerkkinä on puhelinkeskustelu. Varas voi helposti saada tietoonsa jonkin pomon loma-ajat tai milloin hän on paikalla ja milloin ei. Näitä tietoja voidaan hyödyntää esimerkiksi puhelinkeskustelussa esiintymällä hänenä ja etenkin, mikäli esittää olevansa suuressa kiireessä tämän kyseisen asian takia

ja esiintymällä painostavasti. Sihteerikin voi hätääntyä kyseisen asian takia, eikä painostuksen alaisena uskalla hangoitella vastaan kuvitellessaan keskustelevansa pomonsa kanssa ja näin antaakin tiedot suoraan varkaalle.

Toinen vaihtoehto ovat tietomurrot, joissa varas tekee itse ns. likaisen työn. Esimerkiksi hakkeri voi saada tietoonsa yrityksen reitittimen tiedot ja IP-osoitteen, ja mikäli hän pääsee murtautumaan reitittimeen, hän näkee tällöin koko verkon topologian, eli kaikki verkon kytkimet ja laitteet sekä virtuaaliverkot ja kaikkien näiden IP-osoitteet. Tätä kautta voidaan löytää palvelimet ja päästä murtautumaan niille. Mikäli hakkeri pääsee murtautumaan palomuurien ja kytkimien läpi palvelimille ja tätä kautta pääsee tietoihin käsiksi hän voi muuttaa tietoja ilman, että kukaan yrityksestä välttämättä edes huomaa mitään tapahtuneen. Hakkeri voi myös yksinkertaisesti saada kaikki tiedot itselleen, esimerkiksi suuren projektin tarjouspyyntöjen hinnat kilpailijoille tai muuta arkaluontoista materiaalia.

Tietomurtoihin voidaan myös laskea fyysistä turvallisuutta uhkaavat tekijät kuten työpöydälle lojumaan jätetyt asiakirjat tai tuhoamatta jätetyt asiakirjat ja tallennusmediat. Mikäli hakkeri pääsee yrityksen tiloihin tai vaikka vain roska-astioihin, hän voi löytää vaikka mitä tietoa. Asiakirjanippu työntekijän pöydällä sujahtaa äkkiä takin taskuun, tai roska-astioista voi hyvinkin löytää arkaluontoisia dokumentteja, joita ei ole asianmukaisesti hävitetty, puhumattakaan mikäli pääsee käsiksi kokonaisiin dvd-levyllisiin materiaalia, mikä ei ole suojattu. Sama koskee myös kannettavia laitteita kuten puhelimia, pda-käsilaitteita ja tietokoneitakin. Suojaamattomalta kannettavalta tietokoneelta voi äkkiä löytyä mittavia määriä yrityksen arkaluonteista materiaalia, ja tällaisenkin voi vaikka varastaa suoraan henkilöltä itseltään kaupungin ihmisjoukoissa.

2.3 Nykytila

Tietoturva on kehittynyt vuosien saatossa suurin harppauksin ja monista ongelmista, mitkä aiemmin olivat teknisesti vaikeita tai jopa mahdottomia toteuttaa on nykytekniikalla saatu toimivaan tuotantokäyttöön, vähentäen näin käyttäjän omia virheitä luomalla automaatiota. Viruksien, hyökkäyksien ja tietomurtojen kannalta olemme kulkeneet hyvään suuntaan ja niiltä pystytään suojautumaan entistä tehokkaammin, nopeammin ja ennen kaikkea

helpommin. On selkeästi nähtävissä, että jo viimeisen viiden vuoden aikana tietoturvallisuus on kasvanut merkittävästi, paljolti kehittyvän tekniikan ansiosta, mutta ennen kaikkea käyttäjien valveutumisen ansiosta.

Viruksia tehtaillaan kuitenkin tänä päivänä enemmän kuin koskaan, mutta niiltä suojaudutaan entistä tehokkaammin ja kaikki käyttäjät eivät välttämättä edes huomaa oman koneensa koskaan saastuneensa, kun virustorjunta on jo poistanut uhan.

Nykyisin tiedonkalastelu eli phishing on edelleen kaikkein toimivin ratkaisu monissa asioissa, mutta laitteiden ja tekniikoiden kehittyessä hakkerointikin on hyvin yleistä. Viruksien ja matojen ansiosta viruskehittäjät voivat levittää suunnattomat määrät yrityksiä murtautua eri koneille eri puolilla maailmaa äärettömän nopeasti usein käyttäjien itse edes huomaamatta asiaa. Tekniikan kehittyessä hakkereilla ja viruskehittäjillä toki myös tietoturvatekniikat kehittyvät jatkuvasti, mutta usein vasta jälkeen päin. Monissa paikoissa ei ole huomioitu automaattisia päivityksiä, vanhentuneita lisenssejä tai muutoin ei osata antaa riittävää arvoa tietoturva-aukkojen paikkaamiselle. Kaikki nämä auttavat viruksien leviämistä, roskapostin lisääntymistä ja tiedostojen hakkerointia.

3. INFRASTRUKTUURI JA TEKNIIKKA

3.1 Tietoturvan osa-alueet

Tietoturva voidaan jakaa eri osa-alueisiin organisaation ja käyttäjien toimien perusteella seuraavasti:

- hallinnollinen ja organisatorinen tietoturvallisuus
- henkilöstötietoturvallisuus
- fyysinen tietoturvallisuus
- tietoliikenneturvallisuus
- laitteistoturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus
- käyttöturvallisuus

(Viestintävirasto, 2010)

Tässä opinnäytetyössä keskitytään lähinnä infrastruktuuriin ja tekniikkaan, eli laitteiden ja ohjelmistojen turvaamiseen, sillä monien yrityksien kannalta ne ovat kaikkein olennaisimmat tietoturvallisuuden kehittämisen osa-alueet. Työssä esitellään ja käydään läpi niiden perusteita ja joitain painotuksia, mitkä tulee ottaa huomioon oman yrityksen ja politiikan kannalta.

3.2 Perusteet

Kun laitekantaa luodaan tai jo olemassa olevaa otetaan osaksi tietoturvastrategiaa, tulee se merkitä ja luetteloida oikein. Kaikki fyysiset laitteet aina WLAN-tukiasemista palvelimiin ja kytkimiin tulee turvamerkitä ja mielellään valokuvata. Turvamerkinnän voi hoitaa esimerkiksi stanssaamalla laitteen pintaan numero, josta käy ilmi laitteen omistaja ja luettelointitunnus. Valokuvaus on hyödyllinen lisä Poliisille ja vakuutusyhtiötä varten laitevarkauden sattuessa.

Jokainen laite merkitään ja lisätään luetteloon, josta käyvät ilmi kaikkien laitteiden merkintätunnus, sarjanumero, valmistaja ja tyyppi. Samaan listaan voi myös lisätä lisenssien ja takuuajan keston, jolloin listasta tulee tasaisin väliajoin tarkistettuna oivallinen työkalu niiden seurantaan ja uusien hankintaan.

Kaikki verkon aktiivilaitteet tulee suojata lukittuun tilaan tai pienemmässä mittakaavassa lukittuun laitekaappiin. On suositeltavaa käyttää asianmukaisia asennuskaappeja kunnollisella ilmanvaihdolla riittävän jäähdytyksen varmistamiseksi. Näin lisäten laitteiden toimintavarmuutta ja käyttöikää. Kaikki laitteet, joita ei ole tarpeen liikuttaa, kannattaa kiinnittää vaijerilla tukevaan rakenteeseen laitevarkauksien estämiseksi. Monissa videotykeissä, kannettavissa tietokoneissa ja pöytäkoneiden koteloissakin on olemassa valmiina kiinnityskohdat, joilla laite voidaan lukita, ja mikäli laite väkisin revitään irti, kiinnityksen rikkoutuessa se estää laitteen toiminnan ja näin vähentää väärinkäytön riskiä.

Kaikki verkon laitteet, joita ei voida sijoittaa lukittuun tilaan, kuten WLAN-tukiasemat, kannattaa sijoittaa siten, että niihin käsiksi pääseminen vaatii lisätyökaluja, esimerkiksi tikkaat. Tämä lisätyömäärä vähentää potentiaalisen varkaan kynnystä varastaa laite. WLAN-tukiasemien yhteydessä kannattaa myös käyttää POE-toiminnetta (Power Over Ethernet), joka useimmista

nykyaikaisista tukiasemista jo löytyy. POE tarkoittaa sitä, että laite ottaa käyttövirtansa suoraan ethernet-verkosta, johon se on kytketty, eikä näin tarvitse ulkopuolista muuntajaa.

Laitetiloihin tulee järjestää asianmukainen jäähdytys ja ilmanvaihto ylikuumenemisen estämiseksi, ja ne tulee olla aina lukittuna. Laitetilojen oviin tulee olla eri avain kuin muihin yrityksen tiloihin, eikä tätä avainta tule luovuttaa kuin sellaisten henkilöiden käyttöön, jotka sitä välttämättä tarvitsevat. Laitetiloihin tulee myös järjestää asianmukainen sammutusjärjestelmä, mutta kuitenkin siten, ettei se pääse vahingoittamaan laitteita. Esimerkiksi sprinklerijärjestelmä tulee korvata hiilidioksidisammuttimilla, jotka eivät vahingoita sähkölaitteita.

Laiteasennuksia ja huoltoa saa tehdä vain niistä vastaava henkilökunta tai yrityksen valtuuttaman ulkopuolisen huoltoyrityksen henkilökunta, joiden on allekirjoitettava myös salassapitosopimus.

Kaikille laitteille määrätään henkilö, joka on vastuussa laitteen toiminnasta ja oikeasta asennuksesta sekä säilytyksestä. Tämä henkilö on myös vastuussa asianmukaisen huollon järjestämisestä ja valvonnasta.

Kaikki verkon aktiivilaitteet ja työasemat tulee suojata salasanalla ja määrittää käyttäjille vain ne oikeudet, joita he päivittäisessä työskentelyssään tarvitsevat. Ainoastaan verkon ylläpitäjillä tulee olla pääsy aktiivilaitteisiin. Tietoturvastrategiassa tulee myös määrittää salasanapolitiikka. Salasanapolitiikkaan kuuluu mm. salasanan monimutkaisuusmääritelmä. Yleensä käytössä on kahdeksan merkkiä, joista osa on numeroita tai erikoismerkkejä ja osa on suuria ja osa pieniä kirjaimia. Politiikassa myös määritellään mm., kuinka kauan salasana on kerrallaan voimassa, ennen kuin se tulee uusia ja kuinka monta uusintayritystä annetaan, mikäli salasana kirjoitetaan väärin.

3.3 WLAN

Verkkoa suunniteltaessa moni unohtaa, kuinka haavoittuvainen nykyään hyvinkin arkipäiväinen asia kuten WLAN on. Langattomat lähiverkot ovat yleistyneet hyvin nopeasti kaiken kokoisiin yrityksiin helppouden ja edullisuuden vuoksi. Asennuksen ja käytön helppous luo usein myös

turvallisuuden tunteen, ja moni käyttäjä luulee verkon olevan suojassa kaikilta vaaroilta selainkäyttöliittymän iloisesti kertoessa, että verkko on salattu.

Kaikissa WLAN-järjestelmissä on eri tasoisia salasanasuojauksia valittavana sekä monissa myös paljon kehittyneempiäkin turvallisuustoiminteita, kuten vihamielisten tukiasemien tunnistamista (rogue AP), palvelunestohyökkäyksen tunnistamista (DoS) sekä lähetystehon ja suunnan säätämistä. Salasanasuojaus on yksi helpoimmista ja vanhimmista tavoista suojata langaton verkko, mutta erilaisten salasana-algoritmien takia niiden suojaustasot vaihtelevat hyvin suuresti. Tällä hetkellä parasta suojaa tuovat WPA2- ja AES-salaukset, mutta tekniikan edistyessä myös salasana-algoritmit jatkavat kehittymistään.

Nykyään monien laitevalmistajien laitteista löytyy myös muita turvallisuuteen vaikuttavia tekniikoita, kuten DoS ja rogue AP-tunnistukset. Mikäli verkkoa kohtaan tehdään DoS, eli palvelunestohyökkäys, tunnistavat WLAN-tukiasemat tämän välittömästi ja sulkevat sen pois. On myös mahdollista, että vihamielinen tunkeutuja on saanut kaapattua tukiaseman itselleen ja hyödyntää sitä tunkeutuessaan verkkoon, jolloin muut tukiasemat tai WLAN controller huomaa sen, merkkaa tukiaseman vihamieliseksi ja sulkee sen pois muusta verkosta. Näistä toiminteista kirjataan myös tieto logiin ja voidaan antaa hälytys vaikka suoraan verkkovastaavan matkapuhelimeen tekstiviestillä.

Lähes kaikista WLAN-tukiasemista löytyy nykyään myös PoE-tekniikka (Power over Ethernet), joka mahdollistaa käyttövirran syöttämisen tukiasemalle verkkokaapelia pitkin. Tämä vähentää ylimääräisten johtojen tarvetta laitteiden lähistössä ja vähentää laitevarkauden riskiä. PoE-tekniikan käyttöönotto vaatii tämän toiminnon omaavan kytkimen, koska tällä hetkellä vielä kaikki kytkimet eivät oletusarvoisesti sisällä tätä tekniikkaa.

3.4 Verkonvalvonta

Lähiverkon turvallisuuden kannalta on ensiarvoisen tärkeää valvoa kaikkea, mitä verkossa tapahtuu, milloin se tapahtuu ja kuka sen tekee. Monilla laitevalmistajilla on tarjota omille laitteilleen optimoituja ja hyvinkin monipuolisia ohjelmistoja aina logien seurannasta täyteen konfigurointiin, mutta myös erillisiä ohjelmistoja on hyvinkin paljon markkinoilla.

Laitevalmistajien omat ohjelmistot eroavat muista ohjelmistoista siten, että yleensä niissä on parempi tuki ja enemmän toimintoja heidän omille laitteilleen, mutta eivät välttämättä tule toimeen muiden laitevalmistajien laitteiden kanssa. Itsenäiset ohjelmat voivat monesti olla hyvinkin tarkkaan rajattu tiettyyn toiminteeseen tai ovat eräänlaisia ohjelmistopaketteja, joissa on monia työkaluja erilaisten tehtävien suorittamiseen. Itsenäiset ohjelmistot myös tukevat yleensä monien laitevalmistajien tuotteita, mutta joitain ominaisuuksia ei välttämättä aina saa toimimaan, mitä laitevalmistaja lupaa omalle tuotteelleen.

Erilaisilla ohjelmistoilla voidaan seurata mm. verkonliikenne- ja käyttäjämääriä vaikka tiettynä kellon aikana tai viikonpäivänä. Niillä voidaan seurata vikailmoituksia, WLAN-tukiasemien lähetysalueita, liikkuvaa dataa jne. Erilaisia toiminteita on lukematon määrä erilaisiin vaatimuksiin ja erilaisille laitteille, mutta on tärkeää pystyä löytämään itselleen olennaisimmat työkalut. Kaikki verkkolaitteet pystyvät kirjoittamaan logia tapahtumistaan, ja näiden logien seuranta ja tulkitseminen on tärkeää, jotta voitaisiin tunnistaa mahdolliset tietomurrot ja tunkeutumisyritykset. Ohjelmistoilla voidaan logeja seurata keskitetysti nopeuttaen näin prosessia.

Monissa ohjelmistoissa on myös WLAN-verkon suunnitteluun ja ylläpitoon tarkoitettu ominaisuus, johon voidaan ladata yrityksen rakennuksen pohjapiirros, määrittää seinämateriaalit ja näin sijoittaa virtuaalisesti WLAN-tukiasemat ilman varsinaista asentamista. Tämä nopeuttaa langattoman lähiverkon suunnittelua ja vähentää turhan työn määrää. Ohjelmistosta nähdään verkon kantoalue, voidaan määrittää tukiaseman lähetysteho ja joissain malleissa myös lähetyssuunta. Ohjelmistolla voi olla myös mahdollista konfiguroida suoraan tukiasemia ja seurata reaaliajassa verkon toimintaa ja ilmoituksia. Verkon kantoalueen visuaalisesta näkymisestä on hyötyä verkkoa suunniteltaessa, jotta kantavuus riittää yrityksen sisällä kaikkiin tarvittaviin alueisiin, mutta olennaisesti sillä voidaan myös minimoida ulospäin suuntautuva lähetys vähentäen näin yrityksen ulkopuolella verkon kantomatkaa, jolloin verkkoon tunkeutuminen hankaloituu.

3.5 Laitteiden monimuotoisuus

Erilaisilla yrityksillä ja yhteisöillä on kaikilla erilainen ja hyvinkin monimuotoinen laitekanta. Tällä tarkoitetaan sitä, että yrityksessä on käytössä erilaisia työpöytätietokoneita, verkkotulostimia, erilaisia palvelimia, kannettavia laitteita ja monesti myös työntekijöiden henkilökohtaisia laitteita. Mikäli yritys on toiminut vuosia tai jopa vuosikymmeniä, on hyvin mahdollista, että laitekanta on todella monimuotoista ja jo pelkästään työpöytäkoneita voi olla käytössä useaa erilaista. Monimuotoisuus häiritsee tietoturvaa, koska kaikissa laitteissa ei välttämättä voida soveltaa samaa tekniikkaa ja vanhemmat laitteet eivät välttämättä tue kaikkia ominaisuuksia.

Tietoturvallista verkkoa suunniteltaessa kannattaa yhtenäistää laitekanta ja verkkolaitteissa varmistaa laitteiden täydellinen yhteensopivuus, tai mikäli sitä ei voida varmistaa etukäteen, kannattaa suosia saman laitevalmistajan tuotteita toimivuuden varmistamiseksi. Työpöytäkoneilla ei tulisi säilyttää mitään arkaluontoista materiaalia, eikä niitä siten tulisi tarvita varmuuskopioida. Mikäli koneeseen tulee vika, josta ei pystytä toipumaan, vaan kone vaatii uudelleen asennuksen, helpoin tapa on asentaa se levykuvalta.

Kun tietokone on asennettu ns. puhtaalta pöydältä ja laitettu kaikki ajurit ja ohjelmistot toimimaan, siitä kannattaa ottaa levykuva (image). Myöhemmin tällä imagella voidaan asentaa identtinen kopio asennuksesta uudelleen vaikka toiseen koneeseen nopeuttaen prosessia etenkin, mikäli sama paketti tarvitsee asentaa useaan koneeseen. Levykuvalta asentaminen vaatii kohdekokoonpanon olevan identtinen sen koneen kanssa, miltä image on alunperin otettukin, eli tässä tilanteessa tulisi ottaa huomioon työpöytäkoneiden identtisyys. Samaa tekniikkkaa voidaan toki soveltaa kannettaviinkin työasemiin tai jopa palvelimiin varmuuskopion tavoin tai mikäli samanlaisia kokoonpanoja on useita.

Yhtenäiseen laitekantaan sisältyy myös se, että kaikki laitteet voivat käyttää samoja ohjelmistoja. Esimerkiksi kaikkien työasemien tulisi pystyä käyttämään samaa palomuuri- ja virustorjuntaohjelmistoa, samaa selainta ja samaa käyttöjärjestelmää. Tämä siksi, että päivityspakettien jakaminen ja automaattisten päivitysten toimittaminen tapahtuisi kaikille koneille samalla

tavalla, samaan aikaan ja kaikki koneet olisivat samalla turvallisuustasolla vähentäen näin yksittäisen laitteen riskiä toimia verkossa vahingollisella tavalla.

Verkkolaitteiden yhteneväisyys on myös tietyillä alueilla hyvin suotavaa, sillä kaikkien laitevalmistajien laitteet eivätä välttämättä ole keskenään yhteensopivia tai niissä ei ole kaikkia samoja tekniikoita käytettävissä, jolloin voidaan joutua luopumaan tietyistä ominaisuuksista. Myös laitteiden asennus ja konfigurointi voidaan suorittaa useaan laitteeseen helposti samoilla asetuksilla, mikäli kyseessä on saman laitevalmistajan tuotteet, nopeuttaen näin uusien laitteiden implementointia ja vähentäen virheellisten komentojen riskiä tai tiettyjen asetusten unohtamista.

Monilla työntekijöillä voi olla käytössään henkilökohtaisia laitteita kuten älypuhelimia, pda-laitteita tai kannettavia tietokoneita. Näiden laitteiden käyttö yrityksen verkossa tulisi harkita tapauskohtaisesti ja laitteiden tietoturvatasosta tulisi varmistua, ennen verkkoon päästämistä. Mikäli laitetta ei käytetä tuottavan työn tekemiseen, sitä ei tulisi päästää ollenkaan yrityksen tuottavaan verkkoon, vaan pääsy rajattaisiin vierailijaverkkoon, josta ei pääse käsiksi millään tavalla yrityksen tuotantoverkkoihin. Laitteet voitaisiin ohjata karanteeniverkkoon, joka on täysin eristetty yrityksen tuotantoverkosta ja jossa algoritmeillä voitaisiin tarkistaa laitteen tietoturvallisuus. Tarkistuksessa käytäisiin läpi mm. käyttöjärjestelmän versio, uusimmat tietoturvapäivitykset, virustorjunta ja palomuuri. Mikäli havaittaisiin puutoksia, käyttäjä ohjattaisiin päivityssivustolle tai sille voitaisiin lähettää uusimmat päivitykset, ennen verkkoon laskemista.

3.6 Sähköinen turvaaminen

Sähköisellä turvaamisella tarkoitetaan kaikkea turvallisuuteen ja toimivuuden jatkuvuuteen vaikuttavia tekijöitä, jotka johtuvat laitteista tai käytetyistä tekniikoista. Tähän sisältyy mm. viruksilta ja hyökkäyksiltä suojautumista, varmuuskopiointi ja palomuurit.

Varmuuskopiointi on yksi tärkeimmistä toiminnan jatkuvuuden turvaavista tekijöistä ja sen toteuttaminen luotettavasti takaa yrityksen toiminnan jatkumisen, suurienkin tekniikan tai turvallisuuden pettäessä. Mitään yrityksen toiminnan kannalta olennaista tietoa ei tulisi säilyttää työasemilla tai

kannettavilla laitteilla, vaan kaikki tieto tulisi varastoida palvelimille, joiden toiminta on suojattu sähköverkon vikatilanteilta ja jotka on asianmukaisesti varmuuskopioitu. Kaikki olennainen tieto pitää varmuuskopioida ja kaikkia varmuuskopioita tulee säilyttää paloturvallisessa tilassa riittävän kauan, esimerkiksi vuosi varmuuskopion ottamisesta. Kaikkien otettujen varmuuskopioiden toimivuus tulee testata välittömästi, jotta vikatilanteen sattuessa saadaan palautettua viimeisin tieto.

Varmuuskopiointia varten tulee ottaa huomioon yrityksen tarpeet ja kopioitavan tiedon määrä. Pienelle yritykselle saattaa hyvinkin riittää aika ajoin otettu kopio DVD-levylle ja sen säilyttäminen lukitussa, paloturvallisessa tilassa riittävän kauan ja DVD:n säilytys ei vaadi suuria määriä varastotilaa, mutta suuren yrityksen varmuuskopiot saattavat vaatia suuriakin investointeja. Kaikki varmuuskopiot tulee automatisoida siten, ettei inhimillisen unohduksen varaan pääse jäämään yrityksen viikon aikana aikaan saadut työt ja tähän tarkoitukseen on olemassa valmiita ohjelmistoja ja yksinkertaisia menettelytapoja.

Varmuuskopiot tulee ottaa riittävän useasti ja riittävällä tarkkuudella, esimerkiksi tiedostopalvelimen täydellinen varmuuskopiointi kerran kuukaudessa, jota säilytetään 6kk, kerran viikossa tapahtuneet muutokset, jotka voidaan palauttaa täydellisen kopion päälle, säilytetään 2kk ja joka yö otettavat varmuuskopiot, jotka tallentavat muuttuneet tiedostot, jotka voidaan palauttaa viikottaisen varmuuskopion päälle.

Erilaisia ajastustapoja on moneen käyttöön ja jokaiselle yritykselle tulisi suunnitella oma jaksotuksensa sopimaan yrityksen käyttöön, jolloin siitä tulee riittävän tehokas, mutta ei hukkaa tarpeettomasti yrityksen resursseja. Oikeanlaisen ajoituksen löytäminen voi viedä aikaa hioa, mutta näin saadaan turvattua yrityksen materiaalin hukkuminen ja vältyttyä pahimmassa tapauksessa kuukausien työn hukkumiselta.

Erilaisia tallennusmedioita on myös monenlaisia, mutta tällä hetkellä yleisimpiä ovat nauhatallennus, kovalevytallennus ja optiset levyt. Nauhatallennus on tehokas ja ehkä yleisin tapa suuriin tietomääriin tällä hetkellä, mutta laitteiden suurehko investointiarvo pelottaa pieniä yrityksiä. Kovalevytallennus on hyvä vaihtoehto niin keskisuurille, kuin pienillekin

tietomäärille, mutta kustannukset nousevat huomattavasti tietomäärän lisääntyessä. Pienten tietomäärien varmuuskopiointiin optiset levyt, eli DVD ja Blueray levyt ovat edullinen vaihtoehto pienillekin yhteisöille, eivätkä laitteet tarvitse suuria investointeja.

Tulevaisuudessa tekniikoiden kehittyessä on muistettava pitää huoli siitä, että tarvittaessa myös vanhoja varmuuskopioita pystytään lukemaan. Nykyään maailmassa on lukemattomat määrät varmuuskopioitua materiaalia eri yrityksillä, mutta missään ei ole toimivaa laitteistoa, millä niitä voitaisiin avata. Eli on tärkeää säilyttää laitteet toimintakuntoisina ja vanhemman materiaalin siirtämisestä uudelle tekniikalle, jotta sitä voitaisiin tarvittaessa käyttää myös tulevaisuudessa.

3.7 Tiedon salaaminen

Joissain käyttökohteissa on otettava huomioon tiedon salaaminen, eli kryptaus. Kryptaamisella tarkoitetaan tiedon salakirjoittamista siten, että sen lukeminen ja käyttö vaatii esimerkiksi salasanan ja käyttäjätunnuksen. Tämä tekniikka on erityisen hyödyllinen kannettavien laitteiden yhteydessä, sillä kannettavan tietokoneen varastaminen fyysisesti on kuitenkin hyvin helppoa, mikäli kyseessä on liikkuva työntekijä.

Tiedon salaamiseen on olemassa monia ohjelmistoja joiden käyttö on hyvinkin helppoa. Esimerkiksi kannettavaan tietokoneeseen asennetaan ohjelmisto, joka automaattisesti salakirjoittaa koko kovalevyn sisällön siten, ettei sitä pystytä tulkitsemaan ilman asianmukaista käyttäjätunnusta tai tokenia. Token on erillinen laite, joka voidaan liittää vaikka USB-porttiin ja toimii näin käyttäjän tunnistamiseen tai sitä voidaan käyttää erillisen salasana suojauksen tukemiseenkin. Kovalevyn salaamisella vältytään laitevarkauden aiheuttamalta tietoturvariskiltä, sillä ilman käyttäjätunnusta ja/tai tokenia ei tietoihin pääse mitenkään käsiksi.

3.8 Palomuurit ja virustorjunta

Jokaisen yrityksen tietoverkon suojaamisen yhtenä kulmakivenä on palomuuri. Palomuureja voidaan toteuttaa sekä ohjelmallisesti, että ns. rautapohjaisesti erillisellä laitteella. Erillisellä laitteella voidaan valvoa koko verkon liikennettä ja luoda suoraan erityisiä sääntöjä liikenteen ohjaamiseen tai estämiseen. Tämä

on erittäin hyödillinen ominaisuus, kun tarkoitus on suojata verkon aktiivilaitteita ja yleisesti koko verkkoa kerralla. Laitteen asentaminen ja konfigurointi vaatii asianmukaista osaamista ja kokemusta, mutta oikein asennettuna takaa tietoverkon toimivuuden ja vähentää verkossa tapahtuvaa turhaa liikennettä.

Ohjelmistopohjaiset palomuurit on tarkoittu yksittäisten työasemien suojaamiseen ja lisäävät näin henkilökohtaista tietoturvaa. Palomuuriohjelmistot valvovat käyttäjän verkon liikennettä ja varoittavat heti, mikäli epäilyttävää liikennettä havaitaan ja suodattaa suoraan jo tunnettua haitallista tai kiellettyä liikennettä. Myös mikäli palomuuri havaitsee, että uusi prosessi tai ohjelma pyrkii koneelta verkkoon, antaa se hälytyksen ja pyytää käyttäjää selvittämään tilanteen. Ohjelmallisissa palomuureissa on versioita, joita pystyy hallitsemaan suurissakin verkoissa keskitetysti vähentäen verkonhallinnan työtä ja tehostaen toimintaa. Keskitetysti hallinnoimalla kaikkien työasemien ohjelmia voidaan varmistua siitä, että kaikkiin on asennettu viimeisimmät päivitykset ja kaikissa on samanlaiset pääsy ja esto säännöt.

Jokaiseen työasemaan ja kannettavaan laitteeseen tulee asentaa henkilökohtainen virustorjuntaohjelmisto varmistamaan laitteen turvallisuuden. Monet ohjelmistoyritykset tarjoavat yhdistettyä virustorjunta/palomuuri ohjelmistopakettia, jollaisen hyödyntäminen voi vähentää konfiguroinnin määrää ja helpottaa keskitetysti hallintaa. On myös täysin itsenäisiä virustorjunta ohjelmistoja ja niiden valinta on pienissä yrityksissä lähinnä makuasia, mutta vain muutamat ohjelmistot tarjoavat keskitettyä hallintaa, joka on erittäin olennainen palvelu suurille yrityksille. Virustorjuntaohjelmistojen kannalta on ensi arvoisen tärkeää, että automaattiset päivitykset tarkistetaan ja asennetaan päivittäin tai jopa reaaliajassa, sillä joka päivä löytyy uusia haittaohjelmia ja vanhentunut virustutka on niitä vastaan hyödytön.

3.9 Ohjeistus, dokumentaatio ja logit

Yrityksen verkkoa ja tietoturvaa suunniteltaessa tulee järjestää kaikille työntekijöille myös koulutus uusiin menettelytapoihin. Kaikki työntekijät pitää perehdyttää tietoturvallisen käytön perusteisiin, salasanojen oikeaan käyttöön

ja dokumentaation asianmukaiseen käsittelyyn. Monissa yrityksissä on helppoa saada tietoa vaikka paperiroskakorista, joihin on eksynyt arkaluonteista materiaalia, vaikka se tulisi hävittää silppuamalla. Inhimilliset erehdykset ja unohdukset heijastuvat suoraan käyttäjän koulutuksen vajavaisuudesta tai sen puutteesta. Mikäli käyttäjien työskentelyyn tulee uusi lisäys, esimerkiksi uusi tapa hävittää arkistoitu materiaali, tulee varmistua työntekijöiden riittävästä perehdyttämisestä inhimillisten virheiden minimoimiseksi.

Kaikki verkossa tapahtuvista virhetilanteista, tunnistetuista hyökkäyksistä, havaituista viruksista ja koko verkkoliikenteestä tulee dokumentoida. Kaikissa verkon aktiivilaitteissa on dokumentointi ominaisuus, jolloin laite kirjoittaa toiminnastaan logiin. Kaikki laitteiden tuottamat logit tulee käydä aika ajoin läpi, jotta voidaan seurata verkon toimintaa ja varautua sekä suojautua mahdollisia hyökkäyksiä kohtaan. Verkon eri osa-alueiden logeja seuraamalla saadaan tietoa kaikesta mitä verkossa tapahtuu jopa reaaliajassa. Mikäli verkossa havaitaan vieras laite, joka pyrkii jatkuvasti eri tavoilla verkkoon, voidaan se tulkita tunkeutujaksi ja ottaa asiasta selvää.

Myös verkon liikennemääriä seuraamalla voidaan pysyä kartalla, kuinka paljon verkossa oletettavasti keskimäärin liikkuu dataa ja mikäli yht´äkkiä havaitaan suuri poikkeama, voidaan olettaa jotain tapahtuneen. Tällaiset poikkeamat tulee selvittää ja voi olla hyvinkin mahdollista vaikka viruksen päässeen saastuttamaan jonkin työaseman ja lähettää suuria määriä roskapostia tai mainoksia yrityksen työaseman kautta.

Kaikki aiheutuneet vikatilanteet tulee dokumentoida oli syynä inhimillinen erehdys tai tietomurto. Vikatilanteesta tulee selvittää, mitä tapahtui, miksi se tapahtui ja kuinka vikatilanteesta selviydyttiin. Myös suunnitelma ja mahdollinen toteutus siitä, miten vastaavilta uhilta voidaan suojautua tulevaisuudessa. Nämä dokumentoinnit vikatilanteista palautumisesta tulee säilyttää ja tarvittaessa lisätä riskianalyysiin, jotta tulevaisuudessa vastaavanlaisen tapahtuman sattuessa on valmiit toimintaohjeet tapahtuman varalle.

3.10 Fyysinen turvallisuus

Fyysisellä turvallisuudella tarkoitetaan ns. kovan tavaran sekä käyttäjien valvontaa. Perinteisesti fyysistä turvaa luodaan sijoittamalla laitteet ja tieto lukkojen ja ovien taakse sekä valvomalla kulkulupia. Tietoturvapolitiikkaa luotaessa tulee ottaa huomioon erilaiset käyttäjätasot ja niiden kautta eri tilat, joihin käyttäjiä päästetään. Esimerkiksi peruskäyttäjän tunnuksilla ei tarvitse päästä laitetiloihin, joissa säilytetään kytkimiä ja palvelimia.

Laitetilat, joissa sijaitsee verkon rungon muodostavat aktiivilaitteet, reitittimet sekä palvelimet tulee olla aina lukittuja ja niihin tulee olla pääsy vain sitä päivittäisissä työtehtävissään mahdollisesti tarvitsevilla henkilöillä. Kaikkiin yrityksen oviin tulisi asentaa RFID-avaimella toimivat lukot, jolloin työntekijöille ei tarvitse teettää kalliita ns. perinteisiä avaimia ja jolloin pääsyä eri tiloihin voidaan helposti määrittää työntekijäkohtaisesti.

RFID tekniikka on myös edullinen ja nopea ratkaisu yrityksen kaikenlaisten kulkulupien jakeluun ja ylläpitämiseen. Työntekijöiden kulkua voidaan myös seurata vaivatta RFID lukkojen tuottaman lokitiedoston avulla, mahdollisten väärinkäytösten selvittämiseksi. Esimerkiksi laitevarkauden sattuessa voidaan lokeista nähdä, kuka tilassa on viimeiseksi käynyt tai mikäli joku työntekijä kulkee sellaisilla alueilla omilla tunnuksillaan, minne hänen ei kuuluisi päästä.

Laitteet, joita säilytetään yleisissä tiloissa tai ovat muuten helposti saavutettavissa, tulee sijoittaa siten, että niihin käsiksi pääsemiseksi vaaditaan työkaluja, avain tai lisälaitteita. Esimerkiksi WLAN-tukiaseman sijoittaminen kattoon vähentää siihen kohdistuvaa, intuitioon perustuvaa, mielenkiintoa, koska siihen käsiksi pääseminen vaatii tikapuut tai muun korkean esineen, mitä ei välttämättä ole helposti saatavilla. Laitteet tulisi myös mahdollisuuksien mukaan lukita turvalukoilla kiinteisiin rakenteisiin tai muuten suurin huonekaluihin, jolloin niiden liikuttaminen hidastuu huomattavasti. Käytännössä tämä tarkoittaa sitä, että esimerkiksi tietokoneet ja näytöt ja muut vastaavat laitteet tulisi kiinnittää lukitulla vaijerilla paikoilleen, jolloin niiden pois vienti vaatii työkaluja tai asianmukaisen avaimen. Monissa kannettavissa tietokoneissa ja muissa laitteissa on nykyään myös valmis paikka turvalukon asentamiseen, jolloin väkivaltainen laitteen irrottaminen

lukosta, estää sen toiminnan ja näin vaikka itse laite joutuisi vääriin käsiin, ei sen sisältämää tietoa pystytä hyödyntämään.

3.11 Social Engineering

Social engineering on yksi vanhimmista ja edelleen parhaimmin toimivista hakkerointi menetelmistä. Se käytännössä tarkoittaa henkilön harhaanjohtamisella, huijaamisella tai muulla tavoin saatua tietoa. Hakkeri voi hyvinkin esim. puhelimen välityksellä soittaa yrityksen työntekijälle, esiintyä toisena henkilönä ja näin saada tietoonsa asioita, joita normaalisti luovutettaisiin vain yrityksen omille työntekijöille.

Erilaisia tapoja on hyvinkin monia, mutta esim. esiintymällä korkea-arvoisena henkilönä, hyvin röyhkeästi ja esittäen erittäin kiireistä juuri jonkin tietyn asian suhteen saattaa luoda paniikinomaista tunnetta kohde henkilössä, etenkin mikäli kyseessä on työntekijä, joka ei ole ollut yrityksessä kauaa töissä, eikä välttämättä tunne vielä kaikkia yrityksen muita työntekijöitä tai menettelytapoja.

Olemalla röyhkeä, painostaen ja kiirehtimällä saattaa hyvinkin uusi työntekijä luovuttaa yrityksen tietoja ulkopuoliselle, luullessaan keskustelevansa jonkin työnjohtajan kanssa. Kohdatessaan epämiellyttävän, röyhkeästi tai alentavasti käyttäytyvän henkilön, esimerkiksi puhelimessa, ihminen yleensä haluaa päästä hänestä eroon mahdollisimman nopeasti ja tämä on omiaan luomaan painostusta luovuttaa yrityksen tietoja. Työntekijä saattaa luoda nopeasti itselleen mielikuvan siitä, että kyseessä tosiaan on joku yrityksen johtoon kuuluva henkilö ja näin luovuttaa arkaluonteista materiaalia hänelle.

Social engineeringiä voi harjoittaa missä vain ja vaikka yökerhon baaritiskillä tavatessaan kohde yrityksen työntekijän voi hakkeri hyödyntää tämän humala tilaa, esiintyen hyvänä ystävänä, tarjoten muutaman drinkin ja vaivihkaa kysellä tämän työstä ja ehkä näin saaden myös udeltua arkaluontoistakin tietoa.

Suojautuminen tällaiselta hakkeroinnilta voi olla hyvin hankalaa ja parhaiten siihen auttaa työntekijöiden perusteellinen ja oikeanlainen koulutus. Opettaa työntekijät tuntemaan organisaation, jossa työskentelee sekä mitä tietoja saa

luovuttaa kenellekin. Tiettyjä tietoja ei välttämättä saa luovuttaa ollenkaan esim. sähköpostilla tai puhelimitse.

4. TIETOTURVASUUNNITELMA

Tietoturvasuunnitelma on yrityksen yksi tärkeimmistä työkaluista tietoturvan kannalta. Tietoturvasuunnitelma laaditaan jokaiselle yritykselle yksilöllisesti ja yrityksen omat painotukset huomioon ottaen. On ensiarvoisen tärkeää yksilöidä suunnitelma, koska erilaisilla ja eri kokoisilla yrityksillä tarvitaan erilaisia menettelytapoja ja tekniikoita ja yleistyyliset suunnitelmat saattavat hukata tarpeettomasti resursseja tai päin vastoin olla liian niukka suuren yrityksen tarpeisiin. Tietoturvasuunnitelmaa tehtäessä tärkeintä on motivaatio saattaa tietoturva oikealle tasolle ja tiedostaa riskit, joita yritys joutuu kohtaamaan päivittäin ja tulevaisuudessakin.

Tietoturvasuunnitelman aloitusvaiheessa yritykselle määritellään uhat, kuinka vakava uhka on ja kuinka tulee menetellä, mikäli uhka toteutuu. Määritetään myös henkilöt, jotka ovat vastuussa mistäkin aihealueesta tai maantieteellisestä alueesta. Määritellään siis riskianalyysi ja riskien hallinta. Riskianalyysiin yksinkertaisesti listataan mahdollinen uhka, miten se vaikuttaa yrityksen toimintaan, kuinka todennäköinen uhka on, miten siltä vältytään tai kuinka siitä selviydytään. Voidaan myös lisätä kustannusarvio uhan suuruudesta antamaan täsmällisempää tietoa riskistä selviytymiseen. Riskianalyysi määritellään yrityskohtaisesti, koska eri aloilla on erilaisia uhkia ja erilaiset todennäköisyydet uhkien tapahtumiselle. Riskeiltä voidaan myös välttyä ja vähentää niiden todennäköisyyttä hyvin erilaisin tavoin.

Olennaista on oppia ymmärtämään, että vain harva uhka voidaan poistaa kokonaan, mutta riskianalyysiä hyödyntämällä uhka voidaan laskea hyväksyttävälle tasolle. Tämä tarkoittaa sitä, että tiedostetaan riskin olemassa olo, mutta joko kustannuksiltaan tai todennäköisyydeltään se on niin pieni, ettei siihen tarvitse puuttua. Korkean riskin uhissa koko riskin poistamisen mahdollisuus on hyvin epätodennäköistä, joten pyritään vain minimoimaan vahingot.

Kaikista tärkein osa-alue tietoturvasuunnitelmaa tehtäessä on jatkuvuus. Tietoturva ei ole kertakäyttöratkaisu, vaan sitä tulee kehittää ja jalostaa

jatkuvasti. Kun tietoturvasuunnitelma on kerran tehty alusta loppuun kunnolla ja tarkasti, tulee sitä myös aika ajoin tarkistaa ja tarvittaessa muokata uusien tekniikoiden tai tapojen yleistyessä. Tarvittaessa tulee myös päivittää riskianalyysin listausta uusien aiheiden tullessa esiin. Useimmiten kaikkiin riskeihin ei voida varautua ennalta, eikä kaikkia ole mahdollista ottaa huomioon kerralla. Uusien huomioiden tullessa vastaan, pitää kaikki dokumentoida ja listata, kuinka siitä selviydyttiin ja kuinka vastaisuudessa näiltä uusilta uhilta voidaan välttyä tai kuinka riskiä voidaan alentaa. Tietojen pitäminen ajan tasalla on tärkeimpiä tehtäviä toimivan tietoturvan kannalta.

5. TIETOTURVA PROJEKTINA

5.1 Perusteet

Tietoturva on samanlainen prosessi, kuin mikä tahansa muu ICT projekti, noudattaen samaa kaavaa ja toimintaperiaatteita. Kaikki projektit noudattavat keskenään samanlaista kaavaa, ottamatta kantaa, mihin aiheeseen projekti liittyy. Projektissa on aina alku, erilaisia välivaiheita, vaihtoehtoja ja selkeä lopetus. Kaikissa projektin vaiheissa muodostuu jonkinlaista dokumentaatiota, vaiheesta riippuen se voi olla erittäin yleismuodollista, mutta joissain vaiheissa saatava dokumentaatio saattaa olla hyvinkin yksityiskohtaista, esim. tuotespesifikaatio.

Alussa dokumentoidaan projektin lähtökohdat ja suunnitellaan prosessin eteneminen. Määritellään myös vastuuhenkilöt, käydään läpi vaaditut dokumentit, esim. laadunhallinnan kannalta. Erilaisilla välivaiheilla on omat dokumenttinsa ja ne määräytyvät asia kohtaisesti, mutta tällaisia välivaiheen dokumentteja voi olla esimerkiksi tarpeiden kartoituksesta saatu raportti tai pidemmissä projekteissa sen hetkisen tuotannon kattava väliraportointi. Projektin päättyessä luodaan loppuraportti, missä käydään läpi projektin eteneminen, läpi käydyt asiat sekä lopputuote. Viimeinen raportti sisältää kaiken, mitä prosessin aikana käytiin läpi ja saattaa tietyissä prosesseissa olla hyvinkin yksityiskohtainen ja tarkka.

5.2 Prosessikuvaus

Tietoturvan kehittämisen prosessikuvauksessa kerrotaan projektin kulku pääpiirteittäin. Prosessikuvaus on hyödyllinen apuväline tietoturvaprojektin suunnitteluun ja läpiviemiseen, näyttäen selkeästi ja yksinkertaistettuna vastuut, järjestyksen sekä lineaarisen aikajanan.

1) Hallitus ja johtoryhmä tekee periaatepäätöksen tietoturvaprojektin aloittamisesta ja antaa siitä toimeksiannon tietoturvavaltuutetulle. Tietoturvavaltuutettu valmistelee projektin ja kerää tietoa työnjohtajilta eri tarpeista ja painotuspisteistä. Yrityksen eri osastoissa voi olla erilaiset käytännöt jo olemassaan, tässä vaiheessa kaikki tiedot kerätään yhteen ja jäsennellään tulevaa projektia silmällä pitäen. Dokumentaationa nykytilan selvitysraportit.
2) Hallitus ja johtoryhmä suunnittelee ja luo tietoturvapolitiikan, jossa määritellään yrityksen linja tietoturvaa kohtaan. Tietoturvavaltuutettu luo riskianalyysin yritykseen kohdistuvien mahdollisten uhkien määrittämiseksi. Dokumentaationa valmis riskianalyysi sekä tietototurvapolitiikka.
3) Tietoturvavaltuutettu muodostaa tietoturvasuunnitelman ensimmäisen version politiikkaa ja riskianalyysia hyväksikäyttäen sekä käyttäen työnjohdolta saatuja raportteja osastojen tämän hetkisistä menettelytavoista ja käytänteistä. Dokumentaationa tietoturvasuunnitelman kehitysversio.
4) Tietoturvavaltuutettu selvittää mahdolliset investointitarpeet sekä kerää niistä kustannusarvion. Hallitukselle viedään hyväksyttäväksi kyseinen selvitys tarvittavista investoinneista sekä tietoturvasuunnitelman sen hetkinen kehitysversio. Mikäli hallitus ei hyväksy suunnitelman sen hetkistä kehitysversiota, jatketaan seuraavan kehitysversion parissa. Dokumentaationa raportti vaadituista investoinneista.
5) Hallituksen hyväksyttyä tietoturvasuunnitelman kehitys siirtyy tietoturvavaltuutettu määrittelemään koulutushankintoja. Tässä määritellään kuinka yrityksen henkilöstö koulutetaan ja kenen toimesta. Työnjohto sekä henkilöstä koulutetaan tietoturvallisen käyttäytymisen perusteisiin sekä tiedotetaan tulevista muutoksista. Käydään läpi

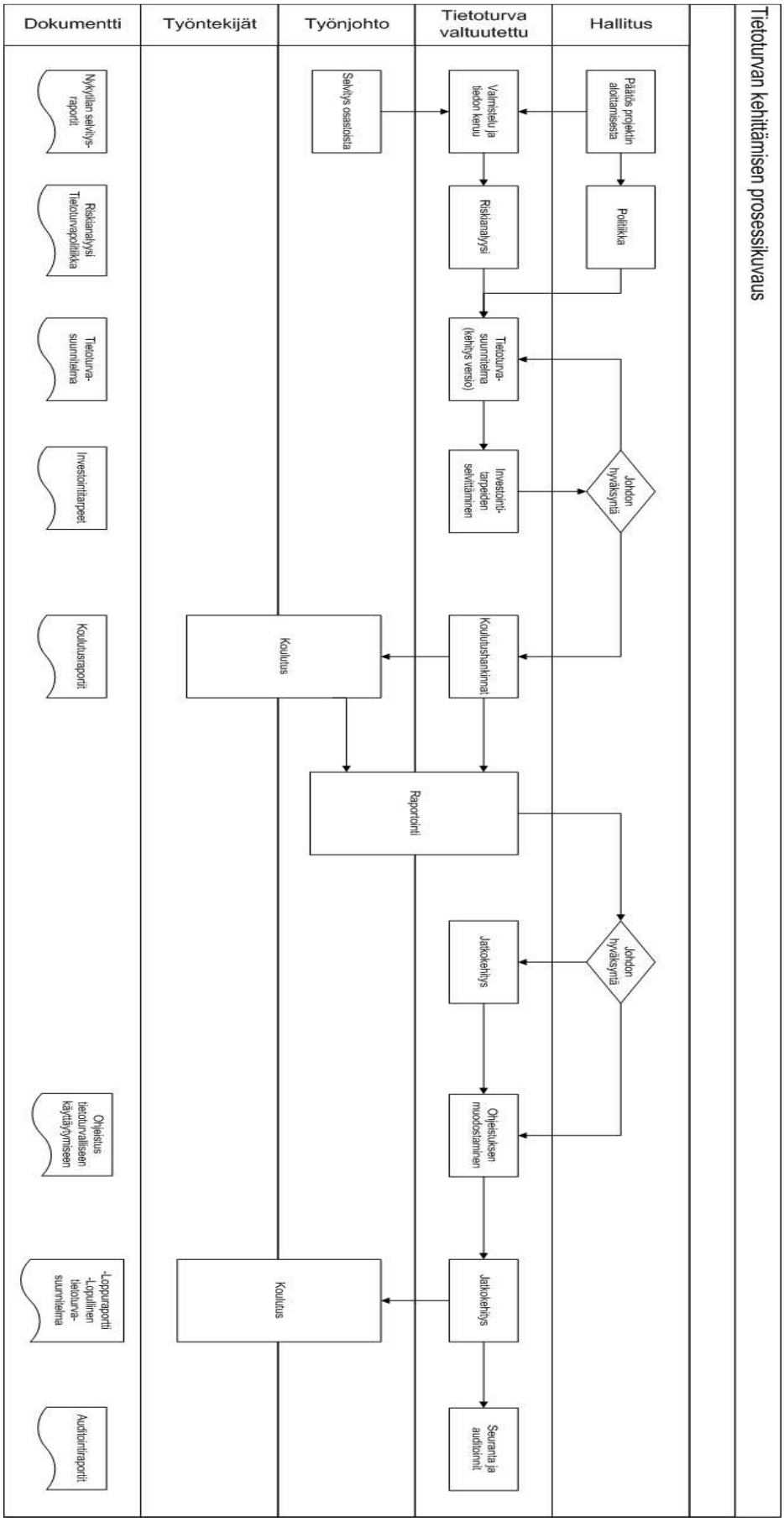
politiikka sekä mahdollisesti kerätään henkilöstöltä palautetta ja kehitysehdotuksia. Dokumentaationa raportit koulutuksien edistymisestä sekä lisäkoulutuksen tarpeista.

6) Tietoturvavaltuutettu kerää väliraportoinnin koko projektin tähän astisesta kehittymisestä, määrittää työnjohdolta saatujen raporttien pohjalta lisäkoulutuksen tarpeen sekä projektin jatkosuunnan.

7) Hallituksen hyväksyttyä esitys muodostaa tietoturvavaltuutettu ohjeistuksen yrityksen koko henkilöstölle, koskien tietoturvallista käyttäytymistä, yrityksen politiikkaa sekä vastuun määrittelyä. Tämä ohjeistus on suurin ja tarkin ohjeistus, joka on tarkoitettu kaikkien työntekijöiden luettavaksi sekä sisäistettäväksi. Kaikki menettelytavat ja periaatteet. Dokumentaationa ohjeistus tietoturvalliseen käyttäytymiseen.

8) Tietoturvavaltuutettu saattaa tietoturvasuunnitelman loppuun, jatkaa järjestelmän kehittämistä sekä vastaa riittävän koulutuksen järjestämisestä työntekijöille. Työnjohto sekä työntekijät koulutetaan, käydään läpi ohjeistus sekä kerrataan politiikka ja mahdolliset riskitekijät. Dokumentaationa projektin loppuraportti sekä lopullinen tietoturvasuunnitelma.

9) Lopuksi järjestetään auditointeja ja seurataan tietoturvan toteutumista yrityksen päivittäisessä toiminnassa. Auditoinnit voidaan järjestää esimerkiksi vuosittain ja mielellään kolmannen osapuolen järjestämänä, puolueettoman näkemyksen takaamiseksi. Tarvittaessa järjestetään koulutustilaisuuksia sekä tarkennetaan ohjeistusta. Riskianalyysin päivittäminen. Dokumentaationa auditointi ja seuranta raportit sekä mahdolliset uudet versiot politiikasta, tietoturvasuunnitelmasta sekä riskianalyysista.



Kuvio 1 Tietoturvan kehittämisen prosessikaavio

5.3 Tietoturvasuunnittelun lähtökohdat

Alettaessa suunnitella yritykselle tietoturvaa on otettava huomioon erilaisia asioita ja mitä erityispiirteitä nämä heijastavat tietoturvaan. On otettava huomioon mm. yrityksen toimiala ja kuinka alalla eri asioita tehdään. On esimerkiksi hyvin erilaista määritellä kaivosyhtiön kannettavien laitteiden turvallisuutta kuin ohjelmistokehitysyrityksen vastaavaa.

Toinen erilaisia valintoja ja ratkaisuja luova aspekti on vanha laitekanta. Onko yleensä vanhaa laitekantaa olemassa, ja jos on, voiko sitä hyödyntää tai miltä osin sitä voisi hyödyntää uudessa projektissa? Monet vanhemmatkin laitteet voivat toimia uudessa ympäristössä hyvin sellaisenaankin tai esimerkiksi käyttöjärjestelmän ja ohjelmistot päivittämällä. Joitain laitteita taas ei voida hyödyntää ollenkaan, ikänsä asettamien rajoitusten vuoksi. Toisia laitteita taas joudutaan korvaamaan mahdollisten rakennemuutoksien takia. Vanhoja laitteita hyödyntämällä saadaan monessa yrityksessä tietoturvan aiheuttamia lisäkustannuksia vähennettyä huomattavasti, säilyttäen kuitenkin riittävän korkean luottamustason.

Uusia laitteita ja järjestelmiä hankittaessa tulee ottaa huomioon yrityksen vaatimukset. Tuleeko esimerkiksi työpöytäkoneita työntekijöille käyttöön kymmenen vai kymmenen tuhatta? Onko verkossa vieraskoneita tai voiko kuka tahansa päästä internettiin yrityksen verkosta mahdollisen vierailijaverkon kautta? Erilaisia asioita tulee siis ottaa huomioon jo olevassa olevien vaatimusten perusteella, mutta tärkeää on ottaa huomioon myös tulevaisuus ja mitä se tuo tullessaan. Kaikki laitteet ja tekniikat kannattaa mitoittaa siten, että mahdollisesti yrityksen ja toimilaitteiden lisääntyessä ei jouduta heti uusimaan laitteita, vaan pystyttäisiin jo olemassa olevilla laitteilla toteuttamaan tarvittavat muutokset näin vähentäen budjetointitarpeita tulevaisuudessa. Esimerkiksi yritykseen ei suunnitella nyt VoIP-puhelinjärjestelmää, mutta sen lisäämistä harkitaan seuraavan kahden vuoden sisällä. Tämä kannattaa ottaa huomioon jo nyt uusia järjestelmiä ostettaessa ja mitoittaessa.

Jokaisella yrityksellä on erilaiset tarpeet järjestelmien suhteen ja pienet verkot ja vaatimukset voidaan toteuttaa hyvinkin pienillä ja yksinkertaisilla ratkaisuilla, mutta nämä eivät taas välttämättä skaalaudu kovin hyvin tai ei ollenkaan

suurissa verkoissa. Suuria ja monimutkaisia järjestelmiä ei taas kannata implementoida pieniin verkkoihin, koska ne varaavat turhaan resursseja ja vaativat suurempia investointeja.

Yrityksen tulee siis määritellä esimerkiksi riskianalyysiä hyväksikäyttäen, mitä he tarvitsevat, minne ja miksi ja millaisia erityisiä painotuksia he mahdollisesti tarvitsevat. Esimerkiksi laitteiden fyysinen turvallisuus voi olla huomattava riski, mikäli moni yrityksen henkilö matkustaa paljon, kun taas paikallaan olevien pöytäkoneiden riski joutua varkauden kohteeksi ei välttämättä ole niin suuri jollekin toiselle yritykselle. Tulevaisuus ja sen tuomat uudet tekniikat tulee myös ottaa huomioon ja miten erilaiset ratkaisut tulevaisuudessa vastaavat kasvavia tietoturvavaatimuksia alati kasvavissa verkoissa ja automaation lisääntyessä.

6. TIETOTURVAPOLITIIKKA

Tietoturvapolitiikka on lyhyehkö, noin yhden sivun kuvaus yrityksen tietoturvasta ja johdon asettamista vaatimuksista jokaisen työntekijän luettavaksi ja ymmärtämiseksi. Tietoturvapolitiikka tulee esittää jokaiselle työntekijälle, tai se tulee muuten saattaa jokaisen työntekijän luettavaksi. Teksti ei ole välttämättä erityisen tarkka kuvaus kaikesta tietoturvaan liittyvästä, vaan pääpiirteittäin selkeästi ilmaistu siten, että jokainen sen pystyy ymmärtämään ja sisäistämään.

Tietoturvapolitiikassa kerrotaan lyhyesti työntekijöille, miksi ohjeistus on luotu ja miten se vaikuttaa yrityksen toimintaan. Tietoturvapolitiikassa määritellään yrityksen aineellinen sekä aineeton omaisuus, kenellä on siihen oikeus milläkin tasolla ja kuka siitä vastaa. Politiikan mukaisesti myös määritellään tietoturvatasot dokumenttien ja tiedostojen käyttöön ja tasosta riippuen määritellään, kuinka kyseinen tieto tallennetaan, kuka sitä saa käyttää, kuinka tietoa tulee kuljettaa ja etenkin, kuinka tiedostot ja dokumentit tulee tuhota. Usein käytössä on kolmen eri tason menetelmä: 1. erittäin luottamuksellinen, 2. luottamuksellinen ja 3. julkinen. Jakamalla tasot johdonmukaisesti saadaan helposti määriteltyä jokaiselle uudelle dokumentille sen vaatimat menettelyt. Henkilöstön ja järjestelmien totuttua uuteen järjestelyyn se nopeuttaa ja yksinkertaistaa yrityksen toimintaa ja yhtenäistää toimintaa.

Tietoturvapolitiikassa tulee tulla ilmi se, kenen vastuulla on työntekijän kouluttaminen tietoturvalliseen työskentelyyn ja miten työntekijä omalla panoksellaan vaikuttaa yrityssalaisuuksien säilyttämisestä yhtiön sisällä ja kuinka se vaikuttaa itse työntekijään. Samalla määritellään, mitä tietoturvallisuudella tarkoitetaan yrityksen kannalta ja kuinka erilaiset uhat saattavat vaikuttaa työturvallisuuteen ja yrityksen toimintaan.

7. TIETOTURVASTRATEGIA

7.1 Hallinto

Olennainen osa tietoturvastrategiaa on sen hallinnointi, kehittäminen ja vastuun määrittäminen. Kuka tai ketkä vastaavat tietoturvan hallitsemisesta, sen kehittämisestä ja kuinka päätökset tehdään tietoturvalliselta näkökannalta. Monesti pelkkä työnjohto ei pysty olemaan mukana tietoturvan hallinnassa, vaan vaaditaan erityinen työryhmä vastaamaan siitä, että tietoturva on ja pysyy ajantasalla. Vanhentunut strategia saattaa pahimmassa tapauksessa vain haitata yrityksen kehitystä, kun taas ajantasainen turvaa myös tulevaisuutta.

Tätä varten tarvitaan hallinto, jonka tehtäviin kuuluu tietoturvastrategian ajan tasalla pitäminen. Hallinto myös määrittää tietoturvapolitiikan mukaisesti vastuuhenkilöt eri alueilla. Mikäli jokin uhka toteutuu tai uusi ilmestyy, jonkun on oltava ensisijaisesti siitä vastuussa ja saatava korjaukset riittävän nopeasti toimintaan yrityksen toiminnan jatkumiseksi. Yleisesti viime kädessä yrityksen tietoturvallisesta toiminnasta vastaa se työryhmä tai henkilö, joka sen määrittää. Pienemmissä asioissa voidaan määrätä työnjohdosta henkilö tai erillinen vastuuhenkilö tietylle alueelle, esimerkiksi työnjohtajan tehtävään kuuluu varmistaa oman osastonsa tietoturvallisesta käyttäytymisestä, koulutuksesta ja osaamistason ylläpitämisestä. Jokainen työntekijä taas omalta osaltaan vastaa omasta tietoturvallisesta käytöksestään tiedon oikeaoppisesta ja määräykset täyttävästä käsittelystä ja hävittämisestä aina yrityssalaisuuksien säilyttämiseen työsuhteen päätyttyäkin salassapitosopimuksen mukaisesti.

Työryhmä tai vastuuhenkilö suunnittelee ja määrittää salassapitosopimuksen, jonka jokaisen työntekijän tulee allekirjoittaa työsopimuksen yhteydessä.

Sopimuksesta tulee käydä ilmi, mitä tietoja työntekijä saa luovuttaa yrityksen ulkopuolelle ja mitkä tulee pitää yrityksen sisällä. Sopimuksesta tulee myös käydä ilmi velvoitteet ja korvausmenettely sekä mahdolliset seuraukset tietojen vuotamisesta. Salassapitosopimus voi olla yksi- tai molemminpuolinen. Yksipuolinen sopimus on tarkoitettu tilanteisiin joissa vain toinen osapuoli luovuttaa luottamukselliseksi määriteltyä tietoa, kun taas molemminpuolinen sitoo kumpaakin osapuolta. Salassapitosopimuspohjia löytyy valmiina, joita on mahdollista yksilöidä yrityksen omiin käyttötarkoituksiin.

7.2 Tietoturvatasot

Kaikille yrityksen dokumentaatiolle tulee määritellä tietoturvaluokitus ja siihen kohdistuvat toimenpiteet tietoturvatasojen määrittelemällä tavalla. Koska kaikessa yrityksen dokumentaatiossa aina kirjepohjista lähtien on potentiaalinen mahdollisuus sisältää arkaluontoista materiaalia, joita ei ole tarkoitettu ulkopuolisille, tulee niille määritellä erilaiset tietoturvaluokitukset.

Tietoturvaluokituksilla ja –tasoilla tarkoitetaan ennalta määrättyä ja sovittua käytäntöä tiettyjen asioiden suhteen. Eri tasoille määritellään se kuka dokumentaatiota saa lukea, muokata, lähettää edelleen ja vastaanottaa sekä selkeät toimenpide ohjeet dokumentoinnin oikeasta hävittämisestä ja varmuuskopioinnista. Koska yrityksillä on liikesalaisuuksia, yrityksen sisällä tapahtuvaa kommunikointia, asiakaspostia ja kaikkea tältä väliltä, tulee kaikki tarkistaa ja merkitä tietylle tasolle. Tietoturvapolitiikan mukainen määritelmä ja yrityksen tietoturvasta vastaava henkilö tai toimikunta määrittelee erilaiset tasot työntekijöiden käytettäväksi.

Monesti käytössä on kolmen tason määritykset: Salainen, luottamuksellinen ja julkinen. Näissä salainen sisältäisi arkoja liikesalaisuuksia, luottamuksellinen yleistä yrityksen sisällä pidettävää arkaluontoista materiaalia ja julkinen kaikkea, mitä asiakkaat ja yleisö pääsee vapaasti tutkimaan. Tasoja voi olla useita erilaisia, mutta ohjeistus tulee olla riittävän selkeä niiden oikea oppiseen käyttöön ja niiden määrityksiä tulee aika ajoin tarkistaa ja tarvittaessa ajanmukaistaa. Jokainen työntekijä vastaa omalla osaltaan tietoturva tasojen asianmukaisesta soveltamisesta ja työnjohdon tulee

määrittää vastuuhenkilö vastaamaan tasojen toiminnasta ja oikea oppisesta kouluttamisesta.

Yleensä asiakirjan luoja päättää dokumentin luottamuksellisuudesta ja siten määrittää sille tarvittavan tietoturvatason. Yleinen ohjeistus kannattaa muodostaa yrityskohtaisesti, omien intressien mukaan ja sitä voidaan soveltaa parhaiten nähdyllä tavalla. Käytännössä ei kuitenkaan ole olennaista, miten viimeisessä piirrossa asiakirjatasoista sovitaan, mutta olennaista on se, että siihen päätetään yksi linjaus, jota kaikki noudattavat. ”Päätetään miten vain, mutta pääasia, että päätetään.”

7.3 Käyttäjien kouluttaminen

Käyttäjien oikea ja asianmukainen kouluttaminen on tietoturvan ja yrityksen yleisen toiminnan kannalta ensiarvoisen tärkeää. Uuden työntekijän tullessa taloon tulee hänet opastaa yrityksen menettelytapoihin ja käytänteisiin riittävällä tasolla, jotta hän pystyy asianmukaisesti toimimaan työtehtävissään. Etenkin tiedon ja mahdollisten laitteiden säilyttäminen ja niiden oikea hävittäminen tulee opastaa kunnolla, ettei arkaluonteista materiaalia päästetä sellaisenaan yleiselle roskalavalle tms.

Uusien tietoturvaratkaisujen ja käytänteiden implementoinnin yhteydessä tulee toimittaa tieto niistä koko henkilökunnalle siten, että ne on mahdollista sisäistää riittävän hyvin ja tarpeeksi etukäteen, väärinkäytösten ehkäisemiseksi. Säännöllisin väliajoin ja tarvittaessa tulee myös järjestää henkilökunnalle koulutustilaisuuksia, joissa kerrataan käytänteet, pyydetään mahdollisesti parannusehdotuksia sekä koulutetaan uusien tekniikoiden ja toimintojen perusteisiin. Parhaallakaan tietoturvatekniikalla ja toimintaperiaatteilla ei ole arvoa, mikäli käyttäjät eivät hallitse niiden käyttöä tai niitä laiminlyödään tuotannollisessa toiminnassa.

7.4 Vastuut

Kuten kaikessa toiminnassa, on myös tietoturvallisuudessa tärkeää määritellä vastuut. Kuka vastaa milläkin tasolla ja kenen puoleen käännytään missäkin tilanteissa? Yrityksessä voidaan luoda täysin oman tyylinen politiikka vastuunmäärittelynkin suhteen, mutta perinteisesti siitä vastaavat työntekijät omalta osaltaan, työnjohtajat omalla alueellaan sekä viime kädessä

toimitusjohtaja sekä hallitus. Yleensä myös kannattaa nimetä erikseen vastuuhenkilö, joka vastaa tietoturvan kehittämisestä sekä auditoinnista. Pienissä yrityksissä tämä henkilö voi myös toimia virassa omien työtehtäviensä sivussa, mutta kuitenkin siten, että aikaa todellakin jää myös tietoturvan kehittämiseen.

Tietoturvallisessa ympäristössä kaikki vastaavat omalta osaltaan tietoturvallisesta käyttäytymisestä ja valvovat sen toteutumista. Kuitenkin perus työntekijä ei voi olla vastuussa muusta kuin omasta toiminnastaan ja vastaa sen toteutumisesta lähimmälle esimiehelleen. Työntekijöiden toisaalta myös työskentelynsä ohella kuuluisi hieman seurata myös mitä heidän ympärillään tapahtuu, eli pääpiirteittäin valvoa esimerkiksi vierailijoiden käyttäytymistä ja mikäli yrityksen tiloissa kulkee tuntemattomia henkilöitä, on aivan hyväksyttävää käydä kysymässä, millä asioilla hän mahtaa liikkua tai ketä hän etsii. Opastamalla vieraat oikeiden henkilöiden luo nopeasti voidaan laskea potentiaalista tietoturvauhkaa.

Kaikkien työntekijöiden vastatessa henkilökohtaisesta toiminnastaan sekä työnsä ohella seuratessa oman työpisteensä lähipiirissä kulkevista vieraista tai tuntemattomista henkilöistä, he raportoivat tarvittaessa ja ovat vastuussa lähimmälle esimiehelleen. Esimiehen tehtäviin kuuluu seurata alaistensa käyttäytymistä myös tietoturvallisuuden kannalta ja tarvittaessa puuttua siihen. Esimies myös vastaa omien alaistensa tietoturvakoulutuksen riittävyydestä sekä opastaa sen noudattamisessa. Tietyin aikavälein kannattaa luoda myös raportti tapahtumista, esimerkiksi kuukausiraportti. Raportissa käsiteltäisiin kuluneen kuukauden tapahtumat, riskit, kehitysehdotukset sekä muut tuotannon tietoturvaan vaikuttavat tekijät. Tämän raportin avulla johtoryhmä sekä tietoturvavastaava voi auditoida ja parantaa turvallisuutta sekä menettelytapoja.

Viime kädessä tietoturvallisesta käyttäytymisestä, koulutuksesta ja auditoinnista vastaavat johtoryhmä sekä hallitus yhdessä tietoturvavastaavien kanssa. Heidän tehtäviinsä kuuluu määräajoin seurata menneitä tapahtumia, niiden vaikutusta yrityksen toimintaan, niistä aiheutuneita toimenpiteitä sekä kuinka tulevaisuudessa vastaavilta tapahtumilta voitaisiin välttyä. Koulutusten järjestäminen aika ajoin kuuluu toimivaan tietoturvaan, sen ylläpitoon sekä kehittämiseen. Tieto auttaa varautumaan ja selviytymään yllättäviinkin

tilanteisiin, mutta vanhentuneena se voi jopa pahentaa tilannetta. Tämän vuoksi onkin suositeltavaa seurata alan kehitystä sekä järjestää esim. vuosittain koulutustilaisuus, missä kerrataan opittua ja perehdytään uusiin menettelytapoihin sekä mahdollisesti uusiin tekniikoihin.

Vastuuta voidaan myös jakaa kolmannelle osapuolelle ja joissakin tilanteissa se on jopa suotavaa. Nykyään on Suomessakin paljon yrityksiä, jotka tarjoavat palveluita yrityksen verkon ja tietoturvan auditointiin sekä tilan selvittämiseen. Myös erilaiset projektiluontoiset järjestelyt, kuten ammattikorkeakoulujen sekä yliopistojen järjestämät koulutus- ja tutkimusprojektit auttavat selvittämään tietoturvan tasoa kustannustehokkaasti.

Mikäli yrityksellä ei itsellään ole tietotaitoa riittävässä mittakaavassa verkkonsa tilan selvittämiseen tai sen ylläpitämiseen, on suotavaa uskoa tehtävä ulkopuolisen tahon hoidettavaksi. Myös aika ajoin ulkopuolisen suorittama selvitys auttaa tehostamaan toimintaa, sillä vaikka yrityksellä olisikin osaava IT-tuki omasta takaa, monesti ihmiset ovat sokeita lähellään oleville tai omille tuotoksilleen. Ulkopuolinen selvitys auttaa puuttumaan näihin epäkohtiin ja nostamaan verkon turvallisuus sille kuuluvalle tasolle.

8. RISKIANALYYSI

Riskianalyysilla tarkoitetaan uhkien ja riskien tunnistamista, niistä selviytymistä sekä niiden ennalta ehkäisyä. Riskianalyysi suunnitellaan ja rakennetaan jokaiselle yritykselle räätälöidysti, sillä vaikka erilaisilla yrityksillä monet uhat voivatkin olla samoja, niiden vaikutukset ja prioriteetti kuitenkin vaihtelevat. Johtoryhmä tietoturvavastaavan avulla selvittää nykyiset uhat yrityksen kannalta, kuinka todennäköistä uhan tapahtuminen on, kuinka se vaikuttaa yrityksen toimintaan sekä henkilöstöön, kuinka uhasta toivutaan ja etenkin, kuinka siltä voidaan välttyä tulevaisuudessa.

Uhan tunnistaminen ja sen olemassa olon myöntäminen on tärkeä osa riskianalyysiä. Esimerkiksi sodan uhka on nykysuomessa hyvin mitätön tällä hetkellä, mutta kuitenkin se tapahtuessaan vaikuttaisi lähes kaikkien yritysten toimintaan. Eri yrityksiin sota vaikuttaisi eri tavoilla, mutta se on selvää, että kaikkiin yrityksiin se vaikuttaisi jollain tasolla, toisiin enemmän toisiin vähemmän.

Uhan määrittelyn jälkeen selvitetään, kuinka todennäköistä on sen tapahtuminen. Vihamielinen tunkeutuminen yritysten palvelimiin on potentiaalinen tietoturva riski lähes jokaiselle yritykselle, mutta toisille yrityksille se voi olla todennäköisempää kuin toiselle. Esimerkiksi pankkien palvelimilla on paljon suurempi riski joutua tunkeutumisen kohteeksi, kuin pikkukaupungin taajaman ruokakaupan palvelimeen.

Seuraava vaihe on selvittää, kuinka uhasta selviydytään, mikäli se on päässyt toteutumaan. Mikäli on selvinnyt, että ulkopuolinen on päässyt yrityksen langatonta verkkoa hyväksikäyttäen tunkeutumaan tuotantoverkkoon ja saanut tuotantodataa itselleen, miten siitä selviydytään? Voidaanko selvittää, kuka on tunkeutumisen takana tai kuinka hän sen teki? Mitä dataa hakkeri sai itselleen ja kuinka tärkeitä liikesalaisuuksia tietoon liittyy? Rikosilmoitus Poliisille ja selvitysten aloittaminen on luonnollinen osa kaikkien varkauksien kanssa, mutta tällaisissa tilanteissa kuuluu selvittää, kuinka tilanteista selviydytään ja miten se pääsi tapahtumaan. Vastaavaisuuden varalle tulee myös selvittää, kuinka uhalta voidaan välttyä tulevaisuudessa tai kuinka sen todennäköisyyttä voidaan laskea.

Riskianalyysin viimeisessä vaiheessa pyritään ennaltaehkäisemään uhkia ja välttämään niiden tapahtuminen. Sotaan ei juurikaan ole monella yrityksellä varaa vaikuttaa, saati estää sen tapahtumista, mutta esimerkiksi tietomurtoihin voi jokainen yritys osaltaan vaikuttaa. Tietomurtojen riskiä voidaan laskea mm. pitämällä käyttöjärjestelmien ja ohjelmistojen versiot ajan tasalla ja tietoturvapäivitykset asennettuina. Myös käyttäjien pääsy tulisi rajoittaa vain heidän tarvitsemiinsa tietoihin jne.

Riskianalyysi ei ole kertasijoituksella valmis. Kun se on kerran suunniteltu ja lähdetty toteuttamaan, kuuluu se pitää myös ajan tasalla ja päivittää tarvittaessa. Mikäli uusia riskejä ilmenee, ne pitää lisätä riskianalyysiin ja selvittää niiden todennäköisyys, selviytyminen ja niiltä turvautuminen. Mikäli jo tiedostetuista uhista toteutuu, päivitetään tietoihin, kuinka siitä selviydyttiin, miten se vaikutti yrityksen toimintaan sekä miten turvallisuutta sen uhan kannalta voitaisiin tulevaisuudessa parantaa.

Taulukossa 1 kuvataan kuvitteellisen yrityksen riskienhallintaa, eli uhkien tunnistamista, todennäköisyyttä, kustannusarviota sekä kuinka niiltä

selviydyttäisiin tulevaisuudessa. Riskianalyysiin voidaan lisätä muitakin ominaisuuksia, jotka koetaan yrityksen kannalta olennaisiksi tai esimerkiksi jakaa riskienhallinta toimialuekohtaisesti.

Esimerkkinä tästä voitaisiin käyttää laitevikaa, joka tietotekniikan osalta voi olla hyvinkin kiusallinen uhka ja lamauttaa pahimmassa tapauksessa koko yrityksen toiminnan moneksi tunniksi, jopa päiviksi. Mikäli laite vika sattuu yrityksen runkokytkimeen, se voi lamauttaa jopa kaiken toiminnan pitkäksikin aikaa, mutta toisaalta yrityksen neuvotteluhuoneen langattoman tukiaseman vikaantuessa, ei tuotanto kärsi ollenkaan, aiheuttaen ainoastaan lievää epämukavuutta palaverin etenemisen kannalta.

Kaikkiin uhkiin ei ole mahdollisuutta vaikuttaa ennalta, mutta niiden todennäköisyyttä on mahdollisuus laskea erilaisten investointien tai toimintatapojen kautta, kuten esimerkiksi varmentamalla kriittiset verkon laitteet UPS varavirta ja jännitesuoja laitteilla tai kahdentamalla sekä luomalla vaihtoehtoisia reittejä ja menettelyitä.

Taulukko 1 Riskianalyysitaulukko, kuvitteellinen yritys

Uhka	Esiintyminen	Kustannus	Hallinta
Tietomurto / hakkerointi	Mahdollinen	Korkea - Erittäin korkea	Ajantasaiset ja oikein konfiguroidut palomuurit, tietoturvapäivitykset, virustorjunta sekä käyttäjien koulutus.
Vesivahinko	Mahdollinen	Korkea	Ei vesisammuttimia laitehuoneisiin, verkon aktiivilaitteet suojataan kaapeilla. Lattiatasossa ei mitään laitteita.
Laitevika	Mahdollinen	Matala - Korkea	Säännöllinen huolto ja tarkistukset, UPS varmennus
Laitevarkaus	Epätodennäköinen	Matala - Korkea	Ei vaadittuja toimenpiteitä.
Virukset / Madot	Todennäköinen	Matala - Keskitaso	Ajantasaiset virustorjunnat sekä palomuurit. Käyttäjien kouluttaminen
Social engineering	Todennäköinen	Matala - Erittäin korkea	Käyttäjien kouluttaminen.
Vakoilu	Epätodennäköinen	Matala - Erittäin korkea	Käyttäjien kouluttaminen. Ajantasaiset palomuurit, pääsynvalvonta
Tietojen luvaton kopiointi omaan käyttöön	Mahdollinen	Korkea	Käyttäjien kouluttaminen, pääsyn valvonta
Yrityssalaisuuksien paljastaminen	Mahdollinen	Korkea - Erittäin korkea	käyttäjien kouluttaminen
Sähkökatko	Mahdollinen	Matala	UPS varmennus kriittisille laitteille
Tietoverkko-hyökkäykset	Mahdollinen	Matala - Keskitaso	Ajantasaiset palomuurit, verkon toiminnan seuraaminen, automaattiset tietoturvapäivitykset

8.1 Riskien vakavuuden määrittäminen

Riskianalyysin muodostamiseen on hyvä käyttää yksinkertaistettua vakavuustaulukkoa, johon määritellään, kuinka paljon tietyn uhan toteutuminen maksaa sekä kuinka todennäköistä se on. Tämän taulukoinnin

perusperiaatteena on luoda vakavuudelle numeroarvo, jonka perusteella voidaan määritellä, kuinka kyseiseen uhkaan suhtaudutaan.

Eli esimerkiksi taulukossa 2 jaamme toteutumistodennäköisyyden neljään osaan, samoin kustannus arvion. Tässä riveille määritellään kustannus arvio ja sarakkeisiin toteutumisen todennäköisyys. Esimerkiksi sähkökatkon todennäköisyys arvioidaan epätodennäköiseksi, mutta tuotannon kannalta jo pienikin katkos aiheuttaa suuret kulut.

Taulukko 2 Vakavuustaulukko

	1. Vähäinen	2. Kohtalainen	3. Suuri	4. Erittäin suuri
1. Epätoden-näköinen			Sähkökatkos	
2. Kohtalainen				
3. Toden-näköinen				
4. Erittäin toden-näköinen				

Taulukon mukaan vaikka sähkökatkoksen kustannukset voivat olla suuret, sen todennäköisyyden ollessa kuitenkin hyvin pieni, muodostuu kokonaisuhaksi pieni. Numeerisesti uhkataso voidaan laskea [todennäköisyys]+[kustannus], eli tässä tapauksessa 1+3=4. Uhkatasot voidaan näin määrittää esimerkiksi taulukon 3. mukaisesti.

Taulukko 3 Esimerkki uhkatasoista

2-4 = pieni	5 = kohtalainen	6-8 = vakava

Kun uhkatasot on määritetty, voidaan luoda yleisohjeistus, kuinka uhkaan suhtaudutaan. Koska kaikkiin uhkiin ei voi ennalta varautua, eikä kaikkia

välttämättä tiedosteta alussa, voidaan yleistää käytäntöä vastaavanlaisiin uhkiin. Esimerkiksi uhka, jonka taso määritellään pieneksi, ei välttämättä aiheuta suoria toimenpiteitä, mutta se kuitenkin tiedostetaan. Uhka, joka määritellään kohtalaiseksi, tulee ottaa huomioon ja määritellä siitä selviytymiseen ohjeistus sekä kuinka siihen tulevaisuudessa varaudutaan. Uhka, joka määritellään vakavaksi, tulee minimoida välittömästi niin kustannuksiltaan kuin todennäköisyydeltäänkin. Eli siltä pitää suojautua parhaalla mahdollisella tavalla ja mahdollisimman nopeasti.

Jokainen uhka, joka tiedostetaan jo alussa, kannattaa käydä läpi taulukon lisäksi tapauskohtaisesti, sillä yleisohje on parhaimmillaankin suuntaa-antava. Vakavuuden määrittämiseen luotu taulukko on parhaiten hyödyksi yleisohjeistuksen tukemana yllättävien tai ennalta tuntemattomien uhkien tullessa esiin. Tällöin saadaan nopeasti määriteltyä, miten uhkaan tulee suhtautua ja siitä toipuminen saadaan nopeasti käynnistettyä. Jälkeenpäin löydetty uhka lisätään riskianalyysiin ja määritellään tarkemmin sekä se, miten uhasta selviydyttiin.

9. RAPORTOINTI JA DOKUMENTAATIO

Nykyään kaikkien yritysten toiminta nojaa vahvasti erilaisiin raportteihin ja dokumentaatioon aina kirjanpidosta tuotantoraportteihin. Näiden raporttien avulla johtoryhmä kehittää yrityksen toimintaa ja suunnittelee toimintamalleja. Raportointi mahdollistaa myös yrityksen nykytilan ja kehityksen seuraamisen sekä tulevaisuuden näkymien ennakoimisen.

Tietoturvan kannalta raportointi ja dokumentaation kerääminen on ensiarvoisen tärkeää, koska se ei ole osana yrityksen ns. fyysistä puolta. Monelle tietotekniikkaan vähemmän perehtyneelle on toisinaan hankala mieltää sen hyödyllisyyttä juuri siksi, ettei sitä varsinaisesti pääse näkemään fyysisenä objektina. Etenkin tietoturvassa asia on hankala, koska ainoa ”fyysinen osa” saattaa olla palomuurilaite jossain laitekaapin perällä, poissa silmistä. Tällöin raportointi ja dokumentaatio on suurin näkyvä osa toimivaa tietoturvaa.

Raporttien avulla voidaan helposti selvittää johtoryhmälle ja työntekijöille tietoturvallisen käyttäytymisen vaikutuksista yrityksen toimintaan sekä kuinka

sitä tulisi kehittää edelleen. Esimerkiksi verkkoliikenteen seurannasta saatavaa dokumentaatiota voidaan luoda raportiksi tietylle aika välille ja sitä kautta seurata, kuinka jonkin tietyn tekniikan, käytänteen tai politiikan implementointi vaikuttaa yrityksen verkkoon ja sitä kautta toimintaan.

Vikatilanteista, turvallisuuspoikkeamista sekä ns. ”läheltä piti” tilanteiden kirjaaminen on yksi tärkeimmistä kehittämistyökaluista. Ilman ajantasaista dataa vikojen yleisyydestä ja ongelmien esiintymisestä, niihin puuttuminen on todella vaikeaa tai jopa mahdotonta. Raportoinnin tarkoituksena on tarjota tietoa tilanteiden kehittymisestä ajan mukaan ja vastata näin kehittyvän ympäristön vaatimuksiin.

Dokumentointi on myös tärkeä osa jatkotoimenpiteiden kannalta esimerkiksi henkilöstön vaihtuvuuden vuoksi. Mikäli tietoturva on lähinnä yhden henkilön harteilla ja olemassa oleva dokumentaatio yrityksen verkosta ja toiminnasta on vajavaista tai jopa puuttuu kokonaan, on uuden työntekijän hyvin vaikeaa selvittää tilanne uudelleen, jolloin yrityksen resursseja sidotaan määrättömästi saman työn tekemiseen moneen kertaan. Dokumentaatiolla varmistetaan toiminnan jatkuvuus myös henkilöstömuutosten tapahtuessa.

Dokumenttien ja raporttien säilyvyys tulisi varmentaa sähköisesti esim. vikasietoisella levyjärjestelmällä ja paperiversioina asianmukaisella arkistoinnilla. Myös dokumenttien arkaluonteisuus tulee ottaa huomioon, sillä tietoturvaraporttien joutuessa vääriin käsiin voi hakkeri päästä käsiksi hyvinkin arkaluontoiseen materiaaliin.

10. TYÖKALUT

10.1 Tarpeiden määrittäminen

Tarpeet tulee määritellä aina yrityskohtaisesti, mutta on seikkoja, jotka ovat kaikille samat. Erilaiset menettelyt vaikuttavat erilaisten yritysten toimintoihin eri tavoin, mutta vaikka toimiala olisi eri, voi jo yrityksen koon mukaan määritellä jotain yhteneväisyyksiä.

Tietoturvan työkaluista perinteisimpiä ja kattavimpia ovat suuret tietoturvastandardit, mutta niiden käyttö ja ymmärrettävyys ei välttämättä aina kohtaa käyttäjien tarpeiden kanssa. Tässä listauksessa on käyty aivan

perustasolta lähtien joidenkin tietoturva-aspektien vaikutus normaaliin työympäristöön mahdollisimman kansantajuisesti ja helposti sisäistettävästi.

Seuraavassa muutamia seikkoja, jotka kannattaa ottaa huomioon ja määrittää miten ne soveltuvat omaan yritykseen. Lista on tarkoitettu suuntaa-antavaksi tarkistuslistaksi, jonka tarkoituksena on auttaa määrittämään yrityksen yleismallisia ratkaisuja tietoturvan ja järjestelmien valitsemisen kannalta. Listassa kerrotaan pääpiirtein, kuinka erilaiset ratkaisut voivat vaikuttaa yrityksen toimintaan, mutta kaikki kohdat tulee kuitenkin arvioida yritys ja tapauskohtaisesti.

1) Mitä palveluja verkolta vaaditaan?
    a. Active Directory.

        Active Directory vaatii palvelimen toimiakseen sekä osaavan ylläpidon. Käytännössä AD vaaditaan jo 10 työaseman verkoissa ja siitä ylöspäin. Hallitsee yrityksen työasemia sekä käyttäjiä.

    b. WSUS

        Windows Server Update Services palvelu vaatii AD palvelimen toimiakseen. Helpottaa yrityksen työasemien ylläpitoa sekä hallinnointia etenkin suurissa verkoissa.

    c. Muuta?
2) Järjestelmien hallinta
    a. Oma hallinnointi

        Vaatii oman ylläpitäjän, riittävällä osaamisella sekä koulutuksella. Osaava järjestelmänhallitsija pystyy luomaan hyvät edellytykset yrityksen IT-infrastruktuurin toiminnalle sekä nopealle vikatilanteista selviytymiselle. Hyvin pienissä yrityksissä ei välttämättä tarvita päätoimista hallinnointia, mutta suuremmissa verkoissa voi tarvita jo useita päätoimisia järjestelmän ylläpitäjiä.

    b. Ulkoistettu hallinnointi

        Ulkoistamalla hallinnoinnin voi yritys varmistaa saavansa aina asiantuntevaa tukea sekä ylläpitoa, mutta joissain tilanteissa

vikatilanteissa palautuminen saattaa kestää omaa IT-tukea kauemmin. Ei välttämättä kustannustehokasta kaikille yrityksille.

3) Työasemien määrä

   a. 1-10

      Ei välttämättä vaadi AD eikä muita verkon palveluita, yrityksen toimialasta riippuen. Verkkolevytila ei vaadi välttämättä suuria investointeja.

   b. 10-50

      AD alkaa olemaan pakollinen palvelu verkon hallinnan kannalta, tietojärjestelmien ylläpito ja kehittäminen vie aikaa ja alkaa vaatia jo päätoimista ylläpitäjää.

   c. 50-200

      Palvelimia voi tarvita jo useita, vaadituista palveluista riippuen. Vaatii päätoimisen ylläpidon ja keskitetyn hallinnoinnin.

   d. 200-

      Vaatii useita ylläpitäjiä, useita palvelimia sekä raskaampia varmennusmenetelmiä. Järjestelmien ylläpito ja kehittäminen vaatii taitoa ja organisointkykyä.

4) Olemassaoleva laitekanta

   a. Hyödynnetään vanhaa

      Joissain tilanteissa vanhan laitekannan hyödyntäminen auttaa pitämään investointikustannukset kurissa ja järjestelmän toiminnassa. Kaikki vanhat järjestelmät eivät välttämättä toimi esim. uudessa käyttöjärjestelmäversiossa, joten joiltain osin vanhojen laitteiden säilyttäminen on vaadittavaa. Vanhan laitekannan elinikä ja tehokkuus ei välttämättä aina vastaa kehittyvän yrityksen tarpeita.

   b. Uusi laitekanta

      Mikäli vanhaa laitekantaa ei ole, tai se uudistetaan kokonaan voidaan varmistua laitteiden tehokkaasta toiminnasta sekä

käyttöiän riittävyydestä. Uudet laitteet ja järjestelmät voivat olla investoinneiltaan mittavia, mutta mahdollisen laitevian tai järjestelmähäiriön riski pienenee huomattavasti vanhaan järjestelmään verrattaessa.

5) Verkon riittävä kapasiteetti

   a. Vanha verkon infrastruktuuri

      Mikäli yrityksessä on jo olemassa oleva tietoverkko ja sitä tullaan hyödyntämään jatkossakin, tulee varmistua sen riittävästä kapasiteetista nyt sekä tulevaisuuden kannalta. Mikäli verkon liikennemäärät kasvavat rajusti, mutta liikennettä hoidetaan liian kevyillä kytkimillä, voi käyttö hidastua huomattavasti ja näin haitata efektiivistä työntekoa. Myös työasemien määrä tulee ottaa huomioon, sillä mikäli kasvun varaa ei ole ollenkaan tai riittävästi, uuden työaseman liittäminen yrityksen verkkoon voi kestää huomattavan kauan uusien verkkojärjestelmien tilauksen ja toimitusaikojen vuoksi.

   b. Uusi verkon infrastruktuuri

      Mikäli vanhaa verkkoa ei ole tai se uudistetaan alusta lähtien, pitää varmistua verkon riittävän kapasiteetin järjestämisestä. Liikennemäärien arviointi ja mittaus auttaa valitsemaan kytkimet ja reitittimet vastaamaan vaadittua kapasiteettia. Myös työasemien määrä tulee selvittää ja arvioida tulevaisuuden tarpeet. Liian vähäinen kytkinporttien määrä ja sitä kautta verkkoon liitettävien laitteiden määrä voi myöhemmin aiheuttaa suurta viivettä tuotannossa tai järjestelmien päivittämisessä.

6) Keskitetty hallinta

   a. Ei keskitettyä hallintaa

      Pienissä yritysverkoissa ei keskitetylle hallinnalle välttämättä ole tarvetta, vaan ylläpito voidaan järjestää työasemakohtaisesti hyvinkin nopeasti. Suuremmissa tai maantieteellisesti laajoissa verkoissa järjestelmien hallinta ja ylläpito vie paljon aikaa, mikäli keskitettyä hallintaa ei ole järjestetty.

b. Keskitetty hallinta

Pienissä verkoissa hyvin marginaalinen hyöty, mutta jo 20 työaseman verkossa hyöty on mittava. Nopeuttaa ja yksinkertaistaa järjestelmien hallintaa ja ylläpitoa suuresti, varmistaen joustavan ja nopean vikatilanteista selviytymisen sekä turvallisen ylläpidon.

7) Varmuuskopioinnin tarve

a. 0-10 Gb

Mikäli varmuuskopioitavan tiedon määrä on hyvin pieni, voidaan se järjestää edullisesti esim. optisille levyille tai SSD-muisteille (ns. muistitikut). Optisten levyjen hyvä puoli on niiden edullisuus sekä helppo varastointi.

b. 10-100 Gb

Yli 10 Gb varmuuskopioinnit vaativat jo kovalevytallennusta tiedon varastoimiseksi. Kovalevy varmennus pienillä tietomäärillä on edullista, turvallista sekä helppohoitoista. Yksinkertaisia RAID-järjestelmiä, esim. peilaus.

c. 100-500 Gb

Kovalevy tallennus on tässä luokassa jo minimi vaatimus. Erilaiset RAID-järjestelmät tulevat ajankohtaiseksi ja erilaiset kovalevytekniikat; SAS / SATA. Nauhatallennusjärjestelmät myös varteenotettava vaihtoehto.

d. 500-1000 Gb

Suuret RAID-järjestelmät useilla kovalevyillä, nauhatallennusjärjestelmät. Alkaa vaatimaan dedikoitua palvelin järjestelmää. Perus kovalevyillä järjestetyt RAID-järjestelmät käyvät hitaiksi ja kustannustehottomiksi.

e. yli 1000 Gb

Suuret levyjärjestelmät tulevat ajankohtaiseksi. Vaaditaan dedikoitua tekniikkaa ylläpitämään varastoitavan tiedon määrää riittävällä tehokkuudella ja varmuudella.

8) Langattomat verkot

   a. Ei ollenkaan

      Mikäli langattomia verkkoja ei ole ollenkaan tai sen hankintaa ei harkita lähitulevaisuudessa, tulee siihen kuitenkin varautua periaatetasolla, sillä tulevaisuudessa yhä useammat järjestelmät vaativat toimiakseen langattomia yhteyksiä.

   b. Pienet, alle 10 tukiasemaa

      Pienien langattomien verkkojen implementointi ja hallinta ei vaadi suuria investointeja, eikä sen ylläpitäminen vaadi suurta omistautumista. Keskitettyä hallintaa ei yleensä tarvita ja perus salasanalla suojatut verkot ovat yleensä riittäviä.

   c. Suuret langattomat verkot

      Suurissa langattomissa verkoissa keskitetty hallinta tulee ajankohtaiseksi ja käytetyt tekniikat tulee järjestää sen mukaan. Halvimmat tukiasemat eivät ole hallittavissa tai niiden ominaisuudet eivät ole riittävät toimivan tietoturvan ylläpitämiseksi, joten investoinnit kasvavat. Myös erillisen WLAN-ohjaimen investointi tulee ajankohtaiseksi verkon ylläpidon ja turvallisuuden kannalta.

9) Koulutuksen järjestäminen

   a. Oma tuki

      Koulutuksen järjestäminen pienessä yrityksessä voidaan hoitaa oman tuen avulla kustannustehokkaasti ja riittävällä tasolla. Tämä kuitenkin vaatii oman tuen riittävää koulutustaustaa, osaamistasoa sekä ymmärrystä tietoturvaa kohtaan. Myös koulutustaidot tulee ottaa huomioon.

   b. Kouluttaja

      Monet yritykset ja järjestelmätoimittajat tarjoavat koulutuspalveluita niin omille tuotteilleen, kuin laajassa mittakaavassakin. Tällaisen kouluttajan tilaaminen voi taata

parhaan oppimistuloksen yrityksen henkilökunnan kannalta, mutta voi konsulttipalkkioiden vuoksi olla hyvinkin arvokasta.

c. Kurssittaminen

Erilaiset oppilaitokset sekä järjestelmätoimittajat järjestävät opetustilaisuuksia eri tekniikoihin sekä yleisiin järjestelmiin. Työntekijöiden kouluttaminen tällaisten kurssien kautta voi olla kustannuksiltaan edullista suhteutettuna opetuksen tasoon, mutta oikeanlaisen kurssin löytäminen ei aina ole helppoa tai niitä ei välttämättä juuri tarvittavalla aika välillä järjestetä.

10) Tietoturvan painottaminen

a. Turvallisuus

Turvallinen painottaminen tarkoittaa tekniikoiden ja menettelytapojen valitsemista vain suojaavuuden kannalta taaten näin järjestelmien ja tietojen turvallisuuden ja oikeanlaisen käytön. Laskee käytettävyyttä aiheuttaen työnteon hidastumista sekä yleistä epämukavuutta.

b. Käytettävyys

Käytettävyyteen panostaminen auttaa työntekijöitä selviytymään nopeasti ja helposti työtehtävistään sekä jättää tietoturvaa paljolti käyttäjän varaan. Altistaa inhimillisille erehdyksille ja sitä kautta tietoturvariskeille. Laskee tietoturvan tasoa ja laskee järjestelmien turvallisuutta.

c. Kompromissi

Käytännössä yksikään yritys ei voi valita vain toista painotustapaa, vaan jokaisen yrityksen on räätälöitävä menettely omien painotuksiensa mukaan ja luotava erilaisia kompromissiratkaisuja tietoturvallisen käyttäytymisen ja käytettävyyden väliltä.

10.2 The Standard of Good Practices

The Standard of Good Practises (SOGP) on Information Security Forumin (ISF) luoma ja ylläpitämä ohjeistus tietoturvan kehittämiseen, hallinnointiin sekä toteuttamiseen yrityksen perspektiivistä. (The Standard of Good Practices 2007)

Standardi pohjautuu muihin tunnettuihin tietoturvastandardeihin (mm. ISO 27002(17799) ja COBIT v4.1), yhdistäen ne selkeäksi kokonaisuudeksi ja tasoittaen mahdollisia näkemyseroja eri standardien välllä. (The Standard of Good Practices 2007)

Useat yritykset käyttävät The Standard of Good Practises:ia työkaluna oman tietoturvallisuutensa kehittämisessä. SOGP toimii työkaluna yhdenlaisena tarkistuslistana, jossa kaikki asiat käsitellään ja perustellaan huolellisesti ja järkisyin yrityksen kannalta. Listaus antaa viitteitä siihen, missä järjestyksessä, miten, kuka ja miksi tiettyjä asioita hoidetaan, kun yrityksen tietoturvaa aletaan suunnittelemaan ja kehittämään vastaamaan tulevaisuuden vaatimuksia.

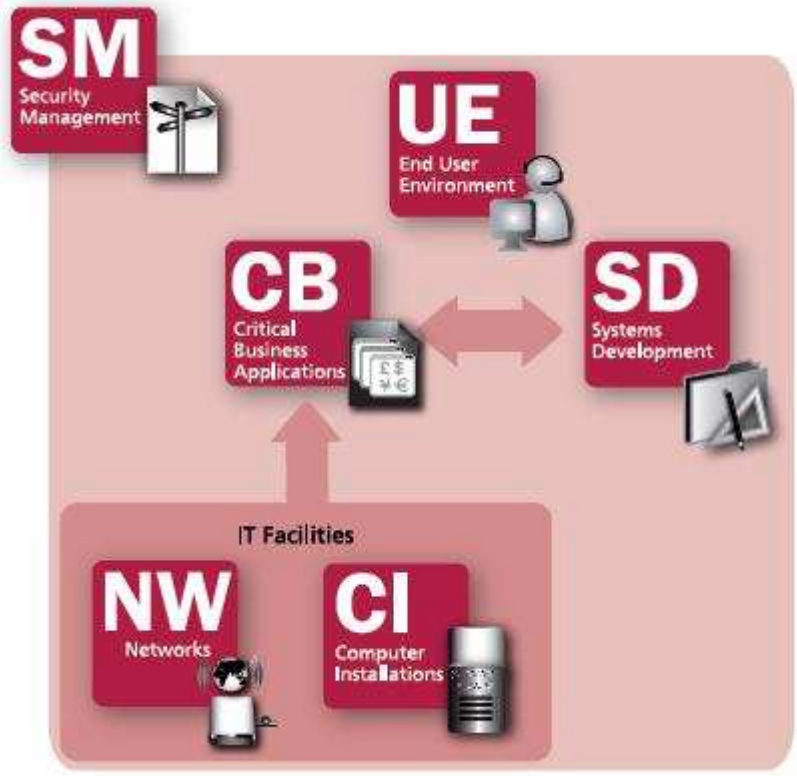
ISF:n the Standard on ensimmäisen kerran julkaistu vuonna 1996 ja sitä päivitetään aina kahden vuoden välein. Päivitykseen sisältyy ajantasaiset käytänteet tietoturvan ylläpitämiseen sekä kyseisen aikakauden ns. "hot topicit" eli ajankohtaiset painotukset. Päivityksissä myös vastataan uusiin yritysten tarpeisiin sekä kehitetään vanhoja tapoja säilyttäen kuitenkin yhtenäisyyden muihin standardeihin. (The Standard of Good Practices 2007)

ISF on kansainvälinen, yli kolmen sadan organisaation yhdistys, jonka kehitysprojekti The Standard on. Jäsenorganisaatiot rahoittavat ja kehittävät itse tätä ohjeistusta kaikkien käytettäväksi. Standardin kehitys perustuu kolmeen pääasialliseen ryhmään; ISF:n oma kehitysprojekti, muiden standardien analysointi sekä suoraan jäsenorganisaatioilta saadut kehitysehdotukset. (The Standard of Good Practices 2007)

SOGP on kokonaisuudessaan vaajaa neljäsataa sivuinen opaskirja, mutta on jaettu selkeisiin alueisiin ja painotuksiin. Teksti on helppolukuista ja hyvin ymmärrettävää sekä painotusalueet ovat selkeitä ja hyvin eroteltuja. Opas jakautuu kuuteen pääkappaleeseen:

- Security Management, joka keskittyy turvalliseen johtamiseen ja on suunnattu yrityksen tietoturvallisuudesta vastaaville henkilöille sekä IT johtajille.
- Critical Business Applications, joka keskittyy yrityksen toiminnan kannalta kriittisien sovelluksien ja prosessien turvaamiseen sekä niiden painotuksiin.
- Computer Installations, keskittyy työasemien ja palvelinten hallinnoimiseen sekä implementointiin. Yleistä järjestelmien asennuksista, hallinnasta ja jatkuvuuden varmistamisesta sekä ennen kaikkea niiden suojaamisesta.
- Networks, tietoverkon suunnitteluun, hallintaan ja implementointiin keskittyvä osa-alue. Turvalliset LAN ja WAN verkot.
- Systems development, sisältää aiheet koko järjestelmän kehittämisestä sekä jatkuvuuden varmistamisesta. Koko järjestelmäkehitys aina suunnittelusta rakentamiseen, testaukseen ja implementointiin.
- End User Environment, antaa ohjeistusta yrityksen paikallisen turvallisuuden järjestämisestä, kannettavista laitteista, tietokantojen ja tiedostojen käytöstä sekä yleistä tietoa lähialueenturvallisuudesta.

(The Standard of Good Practices 2007)



Kuvio 2 Standardin osa-alueiden yhteenliittyvyys

The standard on tehty kenen tahansa saatavaksi ja käytettäväksi, jotta yrityksiin ympäri maailman voitaisiin ajaa yhtenäisiä käytänteitä sekä auttaa yrityksiä pitämään tietoturvansa hyväksyttävällä tasolla myös kansainvälisillä kentillä. Ajatuksena on myös auttaa kehittämään toimintaperiaatteita, jotka ovat käytännöllisiä, keskittyneitä oikeisiin kohdealueisiin sekä vähentävät tehokkaasti erilaisia riskejä. SOGP on suunnattu suurille ja kansainvälisille organisaatioille, mutta siitä on myös todellista hyötyä ja sitä voidaan soveltaa sellaisenaan myös pieniin ja keskisuuriinkin yrityksiin.

(The Standard of Good Practices 2007)

10.3 Windows Server Update Services

Windows Server Update Services, eli WSUS on Microsoftin (MS) ilmaiseksi tarjoama lisäominaisuus Windows Server 2003 ja Server 2008 palvelinkäyttöjärjestelmiin. (Taylor 2009)

WSUS parantaa yrityksen Microsoft ohjelmistojen ja käyttöjärjestelmien tietoturvaa keskittämällä päivitykset ja niiden hallinnoinnin yrityksen omalle palvelimelle ja yrityksen oman järjestelmänvalvojan hallintaan.

WSUS:in toiminta pohjaa Microsoftin omaan päivitystenjakopalveluun, Microsoft updateen siten, että yrityksen oma palvelin käy hakemassa uusimmat päivitykset ja ne jaetaan itse yrityksen sisällä niitä tarvitseville työasemille ja muille palvelimille. (Taylor 2009)

WSUS palvelin tarkistaa automaattisesti MS updaten kautta onko uusia päivityksiä saatavilla, tarvittaessa päivittää oman tietokantansa ja hakee uusimmat päivitykset. Tämän jälkeen järjestelmänvalvoja voi tarkistaa, mitä päivityksiä ajetaan verkon koneille tai jätetäänkö joitain asentamatta. Toisinaan on mahdollista, että MS:n päivitykset saattavat estää tiettyjen ominaisuuksien tai toisien ohjelmistojen toiminnan, joten mikäli tällainen vika on jo ennalta tiedossa, voidaan kyseinen päivitys jättää asentamatta. Järjestelmänvalvojalla on myös mahdollisuus testata asennettavia päivityksiä etukäteen, varmistaen järjestelmien yhteensopivuuden, ennen päivitysten jakamista muille työasemille. (Taylor 2009)

Järjestelmän etuna on em. lisäksi vähentynyt verkon kuormitus. Kun vain yksi palvelin hakee internetin kautta päivitykset, verkon kuorma pienenee huomattavasti verrattuna esim. sadan työaseman vastaavaan päivittämiseen yksitellen. Päivitykset voidaan myös määrittää asentumaan sellaiseen vuorokauden aikaan, kun verkossa ei muutoin ole juuri liikennettä, esim. yöllä, jolloin verkon suorituskykyisyys säilyy silloin, kun sitä eniten tarvitaan.

Verrattuna työasemakohtaisiin, automaattisiin päivityksiin, WSUS järjestelmä nostaa huomattavasti työasemien turvallisuutta, sillä käyttäjät eivät aina muista tai edes viitsi päivittää konettaan, vaikka automaattiset päivitykset neuvoisivatkin käyttäjää asentamaan ladatut päivitykset. WSUS:in avulla nämä päivitykset voidaan keskitetysti pakottaa kaikille työasemille, taaten näin ajantasaiset päivitykset koko verkkoon. Windows Server Update Services siis hakee päivityksiä kaikkiin Microsoftin tuotteisiin, eli käyttöjärjestelmiin, Officeen ja muihin sovelluksiin, minkä päivityksiä jaetaan Microsoft updaten kautta. (Taylor 2009)

Vaatimuksina WSUS:in asentamiselle on Windows Server 2003 tai Server 2008 palvelin, mihin on asennettu Microsoft Internet Information Services (IIS) 6.0, .NET 1.1 SP1 sekä Background Intelligent Transfer Service (BITS) 2.0.

Kokonaisuutena WSUS on yritykselle toimialasta ja järjestelmien mittavuudesta riippumatta erittäin hyödyllinen ja ennen kaikkea ilmainen työkalu, tietoturvan tason säilyttämiseen ja ylläpitämiseen. (Taylor 2009)

11. YHTEENVETO

Tämä opinnäytetyö osoittautui projektina hyvinkin mielenkiintoiseksi haasteeksi osaksi sen mahdollisuuksien, mutta osilta myös sen nykytilaa analysoivan aiheen takia. Aiheeltaan tässä työssä olisi mahdollisuuksia vaikka maan ääriin asti ja vaikeimpia alueita tässä olikin rajata työ sopivaksi, turhaan rönsyilemättä, mutta toisaalta pitää se riittävän kattavana antaakseen kunnollisen kuvan tietoturvan nykytilasta ja kuinka tietoturvasuunnitelmien kehittäminen ja implementointi saadaan onnistumaan sujuvasti perus suomalaisessa yrityksessä.

Aiheen saatuani mietin pitkään ja tarkkaan sitä, kuinka työtä lähtisin kehittämään haluamaani suuntaan, jotta siitä tulisi ns. minun näköiseni ja loppujen lopuksi olen hyvinkin tyytyväinen saavuttamaani tulokseen. Kirjoitusprosessi oli pitkä ja haastava, mutta loppuun myös palkitseva.

Tietoturvallisuuden kehittäminen vaatii jatkuvaa ponnistelua ja uuden oppimista ja tässä työssä käydyt asiat mielestäni auttavat muita tehostamaan omaa oppimistaan ja näkemyksiään tietoturvasta ja sen tarjoamista mahdollisuuksista, mutta myös velvoitteista. Työssä mainitut tekniikat ja käyttäytymismallit tulevat vanhenemaan ajallaan, mutta jotkin niistä tulevat säilymään vielä hyvinkin pitkään. Ne mitkä vanhenevat ja menettävät merkityksensä tulevien vuosien saatossa, toimivat historiatietona ja auttavat tulevaisuudessa ymmärtämään, kuinka asioita on aiemmin tehty, mutta tietoturvallisuudessa uskon, että ajattelumalli tulee säilymään hyvinkin pitkään ja tähän olen myös pyrkinyt tätä opinnäytetyötä kirjoittaessani.

LÄHTEET

Taylor, A. 2009, Windows Server Update Services 3.0 SP2 Operations Guide, Microsoft Corporation

The Standard of Good Practices 2007, Information Security Forum

Viestintävirasto, http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html, Lainattu 17.01.2010